BMC SOFTWARE Certified MarketZone Product

BMC® Performance Manager for Hardware by Sentry Software™

User Guide

Supporting

Hardware Sentry™ Knowledge Module® for PATROL® version 1.3.01 by Sentry Software™

May 8, 2006

Contacting BMC Software

You can access the BMC Software Web site at http://www.bmc.com/. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada		Outside United States and Canada	
Address	BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827	**Telephone**	(01) 713 918 8800
Telephone	713 918 8800 or 800 841 2031	**Fax**	(01) 713 918 8000
Fax	713 918 8000		

Copyright 2006 BMC Software, Inc. or licensors, as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc.

IBM is a registered trademark of International Business Machines Corporation.

DB2 is a registered trademark of International Business Machines Corporation.

Oracle is a registered trademark, and the Oracle product names are registered trademarks or trademarks of Oracle Corporation.

All other trademarks belong to their respective companies.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

Restricted Rights Legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, please see "Before Contacting BMC Software."

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this Web site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and e-mail contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at http://www.bmc.com/support_home.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that Customer Support can begin working on your problem immediately:

- product information
  - product name
  - product version (release number)
  - license number and password (trial or permanent)
- operating system and environment information
  - machine type
  - operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - system hardware configuration
  - serial numbers
  - related software (database, application, and communication) including type, version, and service pack or maintenance level
- sequence of events leading to the problem
- commands and options that you used
- messages received (and the time and date that you received them)
  - product error messages
  - messages from the operating system, such as file system full
  - messages from related software

Copyrights and trademarks

IBM, RS/6000, pSeries, eServer, xSeries, Netfinity, BladeCenter and Director are trademarks or registered trademarks of International Business Machines Corporation.

Fujitsu-Siemens, Primergy and Serverview are trademarks or registered trademarks of Fujitsu-Siemens Computers Corporation.

DELL, PowerEdge, PERC and OpenManage are trademarks or registered trademarks of DELL Computers Corporation.

HP, Compaq, ProLiant, Integrity, SuperDome and Insight Manager are trademarks or registered trademarks of Hewlett-Packard Corporation.

NEC, Express5800 and EsmPro are trademarks or registered trademarks of NEC.

Adaptec and Storage Manager are trademarks or registered trademarks of Adaptec Corporation.

LSI Logic, Mylex and GAM Server are trademarks or registered trademarks of LSI Logic Corporation.

Intel, Pentium and Itanium are trademarks or registered trademarks of Intel Corporation.

AMD and Opteron are trademarks or registered trademarks of Advanced Micro Devices, Incorporated.

Sun and SPARC are trademarks or registered trademarks of Sun Microsystems, Incorporated.

All other trademarks belong to their respective companies.

Contents

Section I - Overview 7
Section II - Getting started 8
1 - How does it work? 9
2 - Integrating Hardware Sentry KM for PATROL 11
3 - The need for vendor-specific hardware monitoring software 12
4 - Using Hardware Sentry KM for PATROL to monitor hardware 13
5 - What sort of hardware can be monitored with Hardware Sentry? 14
Section III - Monitoring 16
1 - Monitoring Temperatures, Fans, Voltages And Power-Supplies 17
2 - Monitoring Storage 20
3 - Monitoring Processors, Memory modules and Network interfaces 22
4 - Missing Device Detection 25
5 - Connector Monitoring 26
6 - Alert Actions 27
Section IV - Configuring and Administering 28
1 - Entering A License Key For Hardware Sentry 29
2 - Distributing the License over Several Computers 31
3 - Temporarily Suspend the Monitoring of an object 32
4 - Terminating Monitoring of a device 33
5 - Restoring the Monitoring of a Device after Removal 34
6 - Choose the way Thresholds are Managed by Hardware Sentry 36
7 - Modifying Parameter Thresholds 38
8 - Pre-Selecting Connectors (optimizing the detection process) 40
9 - Enabling/Disabling Missing Device Detection 42
10 - Setting Security Options 43
11 - Editing Alert Actions 45
Section V - Inside Hardware Sentry 50
1 - Architecture 51
2 - The .HDF files (connectors) 52
3 - The Detection Process 53

4 - The Discovery Process 54
5 - The Collection Process 55
Section VI - Troubleshooting 56
1 - Enabling the Debug Mode 57
2 - Reinitializing Hardware Sentry 58
3 - Hardware Sentry Shows Nothing 59
4 - Unable to See Temperature, Voltage or Fan 60
5 - Unable to See Disk Controller 61
6 - The CPU is overloaded 62

Section I - Overview

Hardware Sentry™ Knowledge Module for PATROL is a BMC Software® PATROL module that allows administrators to monitor the hardware of their servers. Hardware Sentry KM for PATROL is a single KM that is able to monitor the hardware of different server brands: IBM®, HP®, Sun®, DELL®, NEC®, Fujitsu-Siemens® and many others.

Once installed on a PATROL Agent on a server, Hardware Sentry KM for PATROL automatically detects the environment and starts the monitoring of the hardware: status of the disks and the RAID controllers, temperature of the system, speed of the fans, etc.

Section II - Getting started

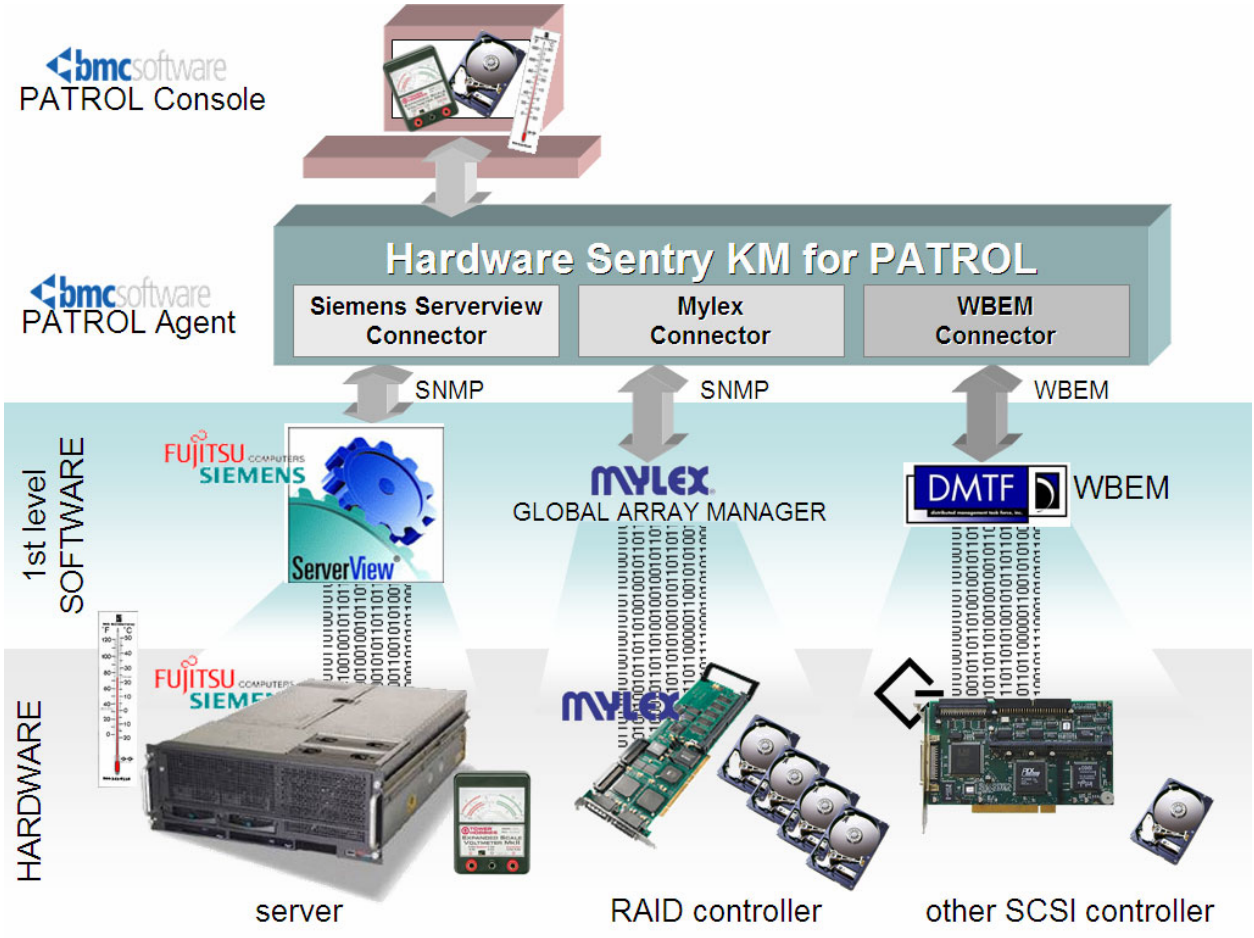
1 - How does it work? 9
2 - Integrating Hardware Sentry KM for PATROL 11
3 - The need for vendor-specific hardware monitoring software 12
4 - Using Hardware Sentry KM for PATROL to monitor hardware 13
5 - What sort of hardware can be monitored with Hardware Sentry? 14

1 - How does it work?

Hardware Sentry KM for PATROL is a module that allows BMC Software PATROL to monitor computer hardware (disk status, temperatures, etc.). It gathers hardware information from different sources (vendor-specific agents, standard management technologies, SNMP, WBEM, etc.) and displays this information within the PATROL framework.

In order to work properly, Hardware Sentry KM for PATROL needs certain hardware information sources to be available. Depending on the platform, Hardware Sentry KM for PATROL will rely on vendor-specific agents and/or on standard management technology such as WBEM or SNMP. On startup, Hardware Sentry KM for PATROL automatically detects which hardware information source is available and then uses this source to monitor the hardware of the computer.

The "big picture" below represents how Hardware Sentry monitors the hardware of a Fujitsu-Siemens® computer. This is a good example to show how Hardware Sentry works:



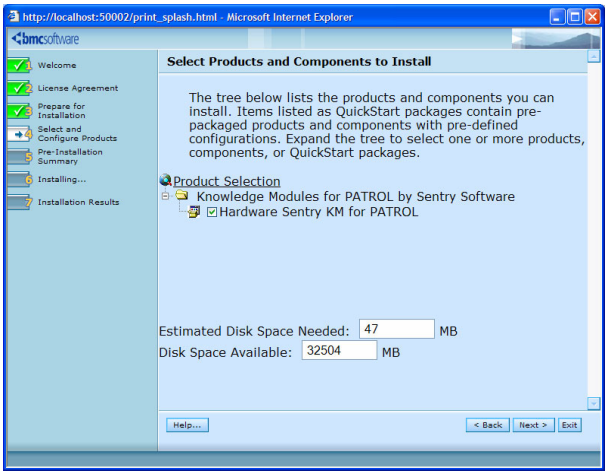
- The Siemens® Serverview® agent shows the temperatures, the fans, the power supplies and the voltages of the Siemens computer through SNMP
- The Mylex® GAM Server shows the status of the physical and logical disks of the Mylex® RAID Controller through SNMP
- The Windows WMI provider shows the status of the physical disks attached to the standard SCSI controller through WBEM
- Hardware Sentry detects and automatically connects to all three information sources (Siemens Serverview, Mylex GAM Server and Windows WMI provider)
- Hardware Sentry gathers the useful hardware information from these sources and displays it within the PATROL framework

Please keep in mind that this is only an example and that it could be applied to IBM, NEC, HP and other computers.

2 - Integrating Hardware Sentry KM for PATROL

Hardware Sentry KM for PATROL is a Knowledge Module (KM) for BMC Software PATROL. Therefore it must be installed on the components of the PATROL framework:

- the PATROL Agents
- the PATROL Consoles
- the PATROL Console Server
- PATROL Central – Web Edition


http://localhost:50002/print_splash.html - Microsoft Internet Explorer
bmcsoftware
Welcome
License Agreement
Prepare for Installation
Select and Configure Products
Pre-Installation Summary
Installing...
Installation Results
Select Products and Components to Install
The tree below lists the products and components you can install. Items listed as QuickStart packages contain pre-packaged products and components with pre-defined configurations. Expand the tree to select one or more products, components, or QuickStart packages.
Product Selection
Knowledge Modules for PATROL by Sentry Software
Hardware Sentry KM for PATROL
Estimated Disk Space Needed: 47 MB
Disk Space Available: 32504 MB
Help...
< Back
Next >
Exit

As any other KM, the active part of Hardware Sentry KM for PATROL resides on the PATROL Agent. A PATROL Agent must be installed on each server which hardware has to be monitored and a copy the Hardware Sentry KM for PATROL must be installed on each PATROL Agent. This version of Hardware Sentry KM for PATROL cannot monitor the hardware remotely.

Once Hardware Sentry KM for PATROL is integrated within the PATROL framework, the hardware information and status of the monitored servers should be available in PATROL.

Please refer to the *Hardware Sentry KM for PATROL – Installation Guide* document for further details on the installation procedure.

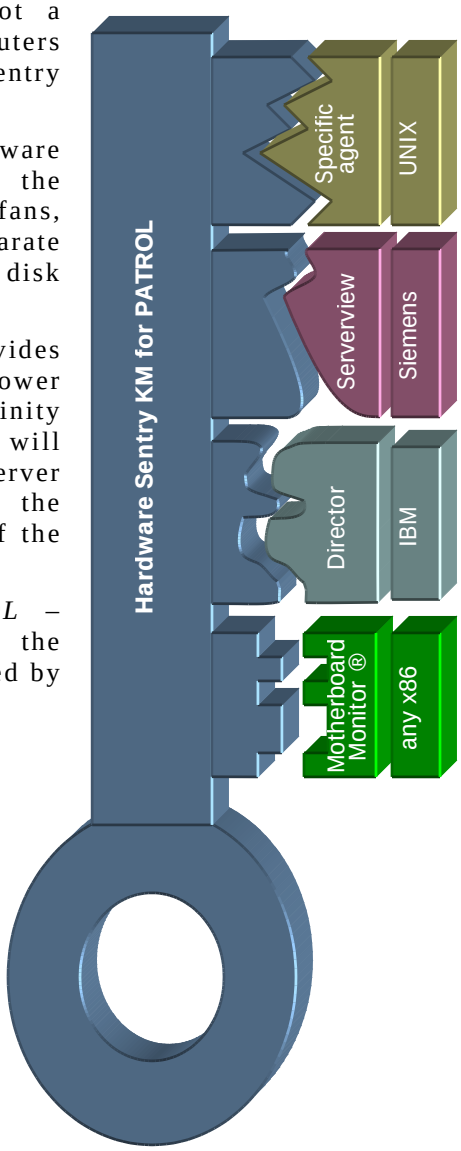
3 - The need for vendor-specific hardware monitoring software

Quite often, the standard operating system layer is not a sufficient hardware information source and most computers require an additional vendor-specific agent for Hardware Sentry KM for PATROL to work properly.

In most cases, server vendors provide the required hardware monitoring agent for their server models. Depending on the platform, a single agent will monitor the temperatures, fans, voltages, power supplies and the RAID systems or a separate agent for the environment monitoring and for the disk monitoring.

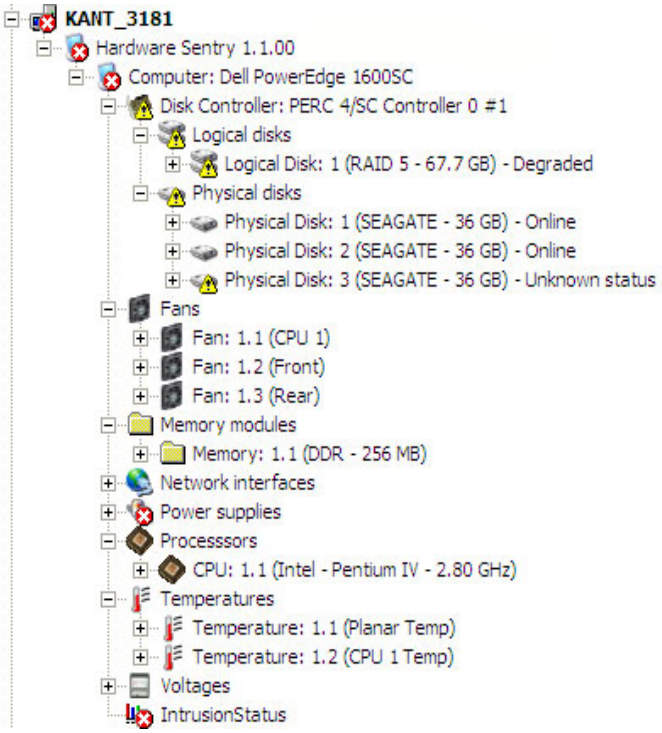
For example, the IBM Director Agent monitors and provides information about the temperatures, fans, voltages, power supplies and ServeRAID disks for IBM xSeries and Netfinity servers. On the other hand, the Siemens Serverview Agent will only monitor the sensors on the motherboard of the server (temperatures, voltages, fans and power supplies) while the Mylex GAM Server monitors the Mylex RAID controller of the server.

Please refer to the *Hardware Sentry KM for PATROL – Installation Guide* document for further details on the installation procedure of the vendor-specific agents supported by Hardware Sentry.



4 - Using Hardware Sentry KM for PATROL to monitor hardware

Once Hardware Sentry KM for PATROL is installed and integrated to the PATROL framework and the hardware information sources are available, the hardware information of the monitored computers will be displayed in the PATROL Consoles (PATROL® Classic Consoles and PATROL® Central). The operators and administrators just have to look at the PATROL Consoles to see the hardware health of their monitored servers in the same way they see the operating system or database health. Under each server icon, a tree represents all the monitored hardware for this server.


KANT_3181
Hardware Sentry 1.1.00
Computer: Dell PowerEdge 1600SC
Disk Controller: PERC 4/SC Controller 0 #1
Logical disks
Logical Disk: 1 (RAID 5 - 67.7 GB) - Degraded
Physical disks
Physical Disk: 1 (SEAGATE - 36 GB) - Online
Physical Disk: 2 (SEAGATE - 36 GB) - Online
Physical Disk: 3 (SEAGATE - 36 GB) - Unknown status
Fans
Fan: 1.1 (CPU 1)
Fan: 1.2 (Front)
Fan: 1.3 (Rear)
Memory modules
Memory: 1.1 (DDR - 256 MB)
Network interfaces
Power supplies
Processsors
CPU: 1.1 (Intel - Pentium IV - 2.80 GHz)
Temperatures
Temperature: 1.1 (Planar Temp)
Temperature: 1.2 (CPU 1 Temp)
Voltages
IntrusionStatus

5 - What sort of hardware can be monitored with Hardware Sentry?

For each supported hardware information source (such as vendor-specific agents or standard technologies), Hardware Sentry KM for PATROL will monitor:

- the status of the disks (RAID and non-RAID disks)
- the speed and/or status of the fans
- the temperatures
- the voltage levels
- the status of the power supplies
- the processors
- the memory modules
- the network interfaces

Actually, Hardware Sentry KM for PATROL does not support hardware platforms but hardware information sources. Currently Hardware Sentry KM for PATROL supports the following hardware information sources:

- Adaptec Storage Manager (both Standard and Browser Editions)
- Dell OpenManage Agent under Windows and Linux
- Fujitsu-Siemens Serverview Agent under Windows and Linux
- Fujitsu-Siemens BX300/600 Management Module
- HP NetRAID SNMP sub-agent under Windows
- HP Management Agents under Windows, Linux and Tru64 (HP TopTools and HP Insight Manager Agent)
- HP-UX standard monitoring tools
- IBM Director Agent 3.1, 4.1 and 4.2 under Windows and Linux
- IBM BladeCenter Management Module
- IBM RS/6000, pSeries and eServer p5 standard tools under AIX
- LSI Logic Power Console
- Motherboard Monitor® (licensed by Alexander van Kaam, mbm.livewiredev.com)
- Mylex GAM SNMP sub-agent under Windows
- NEC ESMPRO Agent under Windows
- Sun standard hardware monitoring tools under Solaris
- WMI under Windows (S.M.A.R.T. disks and network interfaces)

Therefore, Hardware Sentry KM for PATROL is able to monitor the following platforms that are supported by the information sources above (non-exhaustive list):

- Dell PowerEdge servers under Windows and Linux
- Fujitsu-Siemens Primergy servers under Windows and Linux
- Fujitsu-Siemens Primergy Blade servers
- HP (Compaq) ProLiant servers under Windows and Linux
- HP NetServer servers under Windows only

- HP 9000 servers under HP-UX
- HP AlphaServer servers under HP Tru64 UNIX
- IBM xSeries servers under Windows and Linux
- IBM Netfinity servers under Windows only
- IBM BladeCenter
- IBM RS/6000, pSeries and eServer p5 under AIX
- NEC Express5800 servers under Windows
- Sun Ultra and Fire servers under Solaris
- any PC with non-RAID, IDE or SCSI and SMART-capable disks
- any PC with standard sensors supported by Motherboard Monitor®

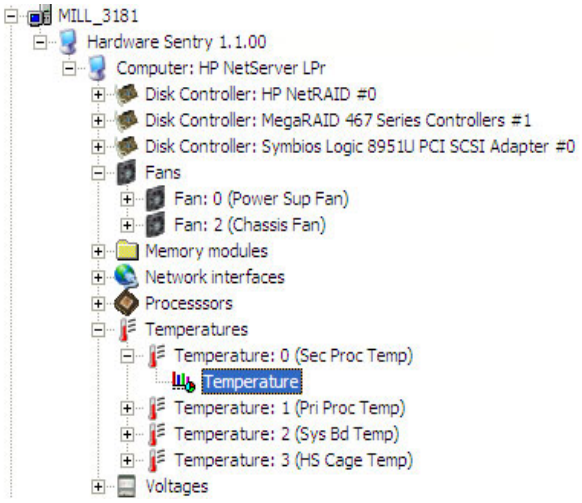
As Sentry Software is continuously working on the support of new hardware information, sources and new platforms that can be monitored with Hardware Sentry KM for PATROL will continue to grow.

Please check our web site (www.sentrysoftware.net) to find the latest updates. Add-ons for Hardware Sentry KM for PATROL can be obtained for free and do not need an update of the KM itself.

Section III - Monitoring

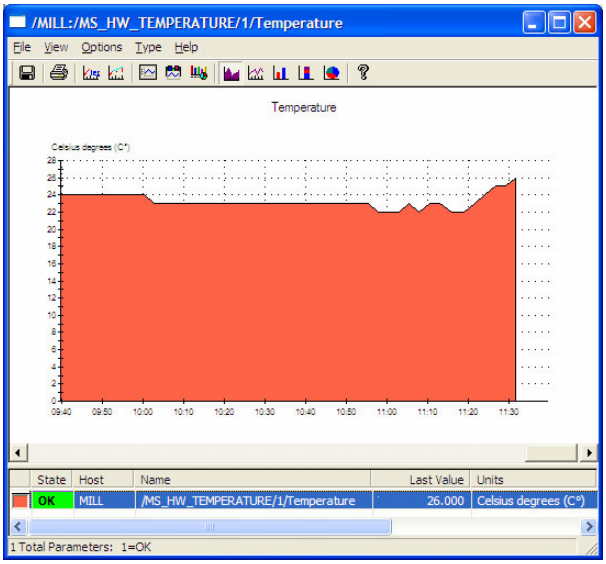
1 - Monitoring Temperatures, Fans, Voltages And Power-Supplies 17
1.1 - Fans 18
1.2 - Temperatures 18
1.3 - Power Supplies 18
1.4 - Voltages 19
2 - Monitoring Storage 20
2.1 - Disk controllers 20
2.2 - Physical Disks 20
2.3 - Logical Disks 21
3 - Monitoring Processors, Memory modules and Network interfaces 22
3.1 - Processors 22
3.2 - Memory Modules 23
3.3 - Network Interfaces 23
4 - Missing Device Detection 25
5 - Connector Monitoring 26

1 - Monitoring Temperatures, Fans, Voltages And Power-Supplies



Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If a hardware information source provides useful data about temperatures, fans, voltages or power-supplies, an icon is automatically created for each sensor found in the system as well as one or more parameters.



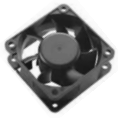
For each displayed sensor, one or more graphs are built by polling the sensor every two minutes. These graphs can be viewed by double-clicking the parameter under the corresponding icon in the PATROL Console.

The location or the type of the sensor may appear in the icon label if this information is available as well.

Depending of the platform and sensors and if possible, alert thresholds are automatically set by Hardware Sentry KM for PATROL. When the parameter value reaches these thresholds, the parameter triggers a warning or an alarm and this alert is sent by the PATROL Console to the operators and administrators.

Note: If a device appears to be missing, the “Status” parameter will be used to trigger an alert.

1.1 - Fans



To avoid temperatures that are too high, system vendors install fans on critical devices (processors, power supplies, etc.). Monitoring fans is important because they ensure a proper temperature for the system to work efficiently.

Depending on the available information, the *Speed* and/or *SpeedPercent* and/or *Status* parameters will be displayed for each detected fan device:

- The *Speed* parameter represents the speed of the corresponding fan in rotations/minute. An alert is triggered if the fan speed is too low for proper functioning.
- The *SpeedPercent* parameter represents the speed of the corresponding fan in percentage of its maximal speed. An alert is triggered if the fan speed is too low for proper cooling.
- The *Status* parameter represents the current status of the fan. An alert is triggered if the fan stops spinning or does not spin fast enough.

1.2 - Temperatures

As with any electronic device, chips and other components of a computer stop working when their temperature rises too high (lots of unrecoverable errors, crashes and even hardware hurt). This temperature may become too high when the device is abnormally overloaded, when a fan is not working properly or when the ambient temperature is too hot. Monitoring the temperatures of the critical devices of your system allows you to take action before a crash occurs.

Depending on the available information, the *Temperature* and/or *Status* parameters will be displayed for each detected temperature sensor:

- The *Temperature* parameter represents the current temperature reading in Celsius degrees (°C). An alert is triggered if the temperature becomes too high.
- The *Status* parameter represents the current status of the temperature. An alert is triggered if the temperature gets too high.

1.3 - Power Supplies

The power supply is the component that transforms the AC Line into electric power needed by the computer. Therefore the power supply is a highly critical device of a computer that should never fail. Due to this, many vendors build servers with redundant power supplies. Monitoring power supplies allows the operators to be alerted when a power supply fails, or even in some cases when a power supply is overloaded.

Depending on the available information, the *UsedCapacity* and/or *Status* parameters will be displayed for each power supply or power unit device:

- The *UsedCapacity* parameter represents the power supply's power currently in use as a percentage. An alert is triggered when the power supply's maximum power output is reached.
- The *Status* parameter represents the current status of the power supply. An alert is triggered if an error occurs with the power supply.

1.4 - Voltages

Power supplies convert the AC line power into voltages and currents needed by the motherboard of the computer. The stability of the motherboard (and therefore of the overall computer) strongly depends on this power converter. Voltages that are too low or too high may lead to unpredictable system crashes. Monitoring the value of the different voltages needed by the motherboard will help in detecting unstable system instability.

Depending on the available information, the *Voltage* and/or *Status* parameters will be displayed for each voltage sensor on the motherboard:

- The *Voltage* parameter represents the voltage output in milliVolts (mV). An alert is triggered if the voltage goes out of the proper range.
- The *Status* parameter represents the current status of the voltage. An alert is triggered if the voltage output is too low for proper functioning.

2 - Monitoring Storage

Disk Controller: Adaptec AIC-7899 Ultra160/m PCI SCSI Card #0
Physical disks
Physical Disk: 0 (SEAGATE ST39175LW SCSI Disk Device
Disk Controller: Mylex DAC960ptl1 #0
Logical disks
Logical Disk: 0.0 (RAID 1 - 8.5 GB)
Physical disks
Physical Disk: 0.0.0 (SEAGATE - 9 GB) - Dead
Physical Disk: 0.0.1 (SEAGATE - 9 GB)
Physical Disk: 0.0.2 (SEAGATE - 9 GB)

Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If at least one hardware information source provides useful data about the storage in the computer, an icon will be created for each storage-related device in the PATROL Console: disk controllers, physical disks and logical disks.

Physical and logical disks icons are created below the disk controller icons they are attached too. Each icon is labeled with a description of the device: ID, size, vendor, role, etc.

Note: If a device appears to be missing, the “Status” parameter will trigger an alert if necessary.

2.1 - Disk controllers

A disk controller is a card inside a computer that connects one or several physical disk drives to this computer. Some intelligent disk controllers (such as RAID controllers) manage several physical disks as a single logical disk which is the only disk exposed to the operating system. Monitoring both physical and logical disks is essential to ensure that storage is available.

Disk controllers do not have a parameter and no information about them is collected. Their sole purpose is to graphically represent how the disks are arranged in the computer. Please note, however, that if a controller goes missing, all its disk dependencies will be missing as well.

2.2 - Physical Disks

Physical disks must be monitored to avoid loss of data, unavailability and performance degradation. When available, the S.M.A.R.T. technology will be used to predict a disk failure before it occurs.

Depending on the available information, the *PredictedFailure*, *ErrorCount* and/or *Status* parameters will be displayed for each discovered physical disk:

- The *PredictedFailure* parameter uses the S.M.A.R.T. technology to predict physical disk failures. An alert will be triggered if it is predicted that the Physical Disk will soon break down.
- The *ErrorCount* parameter is incremented each time an error occurs on this physical disk. An alert is raised from the first detected error. The operator can reset the counter and clear the alert through a Menu command in the PATROL Console.
- The *Status* parameter represents the current status of the physical disk. An alert is triggered if the physical disk is not available for proper operation.

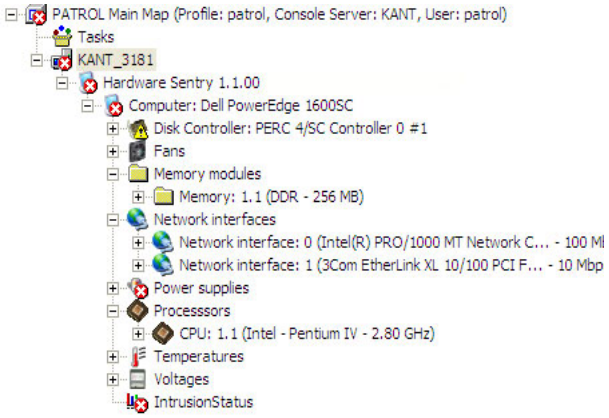
2.3 - Logical Disks

RAID or advanced disk controllers expose several physical disks as a single logical disk to the operating system. The status of a logical disk typically corresponds to the status of a RAID array (on-line, degraded, rebuilding, etc.). For each logical disk discovered, the *Status* parameter is displayed:

- The *Status* parameter represents the current status of the logical disk. An alert is triggered when the logical disk is not fully operational (degraded, rebuilding, etc.) or not available at all.

Note: For non-RAID disk controllers (as most of IDE controllers, for example), no logical disk will be displayed.

3 - Monitoring Processors, Memory modules and Network interfaces


PATROL Main Map (Profile: patrol, Console Server: KANT, User: patrol)
Tasks
KANT_3181
Hardware Sentry 1.1.00
Computer: Dell PowerEdge 1600SC
Disk Controller: PERC 4/SC Controller 0 #1
Fans
Memory modules
Memory: 1.1 (DDR - 256 MB)
Network interfaces
Network interface: 0 (Intel(R) PRO/1000 MT Network C... - 100 Ml
Network interface: 1 (3Com EtherLink XL 10/100 PCI F... - 10 Mbp
Power supplies
Processsors
CPU: 1.1 (Intel - Pentium IV - 2.80 GHz)
Temperatures
Voltages
IntrusionStatus

Hardware Sentry automatically detects the information sources available on the monitored computer and displays the hardware information provided by those sources in the PATROL Consoles in the corresponding container.

If at least one hardware information source provides useful data about the most critical non-storage devices in the computer, an icon will be created for each device in the PATROL Console: processors, memory modules and network interfaces.

Processors, memory modules and network interfaces icons are created under a computer icon. Each icon is labeled with a description of the device: ID, size, vendor, role, etc.

Note: If a device appears to be missing, the “Status” parameter will trigger an alert if necessary.

3.1 - Processors

Processors (also called CPU, Central Processing Unit) are obviously the most critical devices within a computer. While a processor fault may often lead to a system crash without a chance for a monitoring tool to catch the error, it can still be useful to monitor a server’s processors.

In the case of a system crash due to a processor fault, the system reboots automatically. The reboot is either triggered by the operating system or by the motherboard itself. If a processor is no longer working, it is automatically disabled by the BIOS and, if there is one processor left, the operating system starts with one processor less.

Hardware Sentry monitors each processor and checks that it is present and running. If a processor is missing upon a reboot, Hardware Sentry will trigger an alert.

On some recent or high-end servers, processors are able to correct some operation errors by themselves (like the ECC memory). If this information is available, it is shown in the PATROL Console by Hardware Sentry. In addition, if the processor is able to predict a future failure this information will be monitored by Hardware Sentry and shown in the PATROL Console.

Depending on the information available, the *Status* and/or *CorrectedErrorCount* and/or *PredictedFailure* parameters will be displayed for each discovered processor (CPU):

- The *Status* parameter represents the current status of the processor. An alert is triggered if the processor is not available for proper operation (missing, disable by the BIOS due to a POST error, etc.).
- The *PredictedFailure* parameter reports the predictive failure analysis, performed by the processor itself. This information is based on the rate of corrected errors.
- The *CorrectedErrorCount* parameter represents the number of errors that have been automatically corrected by the processor. This information can be very useful to predict a failure in the near future.

3.2 - Memory Modules

The main memory of a computer is actually as critical as the processors since almost all processor operations deal with the memory. A single memory fault will lead to severe computer crash with, potentially, data corruption. On servers, the memory modules (the devices where the memory data is actually stored) often include auto-correction features (ECC), and sometimes even better: RAID5-like memory configuration. These features and configurations allow the memory modules to report statistics on failures, to predict failures, to hot-replace a memory module upon failure, etc.

Depending on the available information and the features provided by the motherboard and the memory modules, the *ErrorCount* and/or *PredictedFailure* and/or *Status* parameters will be displayed for each discovered memory module:

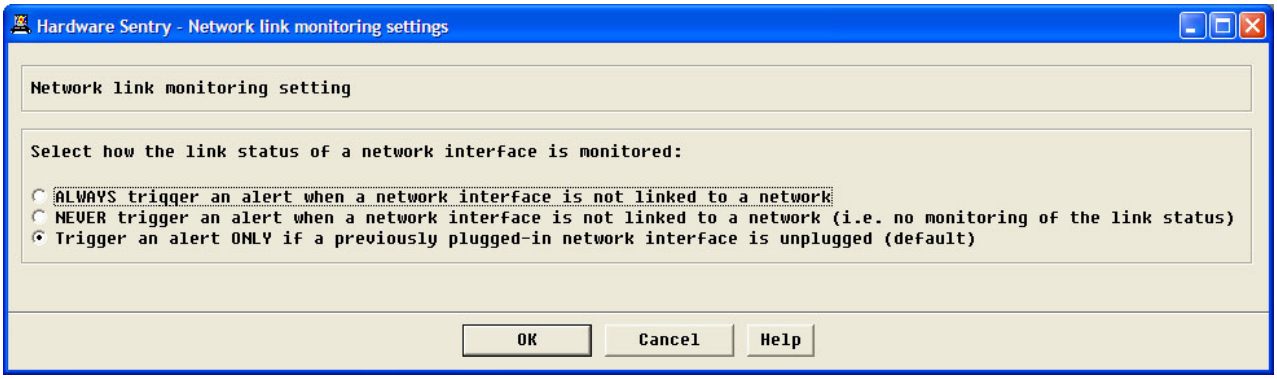
- The *ErrorCount* parameter reports the number of errors that have been detected by the memory module and then corrected. A steadily growing value means that the memory module is not reliable and that it could encounter errors that it is unable to correct and that will then crash the system.
- The *PredictedFailure* parameter is reported by the memory modules which try to predict if it is going to fail by analyzing the trend of the number of detected/corrected errors (thanks to the ECC technology). If this parameter goes into alarm, you should remove the faulty memory module and replace it with a new one.
- The *Status* parameter represents the current status of the memory module. An alert is triggered if the memory module reports a failure (in a RAID5-like configuration) or if it is missing after a computer reboot.

3.3 - Network Interfaces

Network interfaces are devices that serve as a common interface for various other devices within a local area network (LAN), or as an interface to allow networked computers to connect to an outside network. It is therefore essential to make sure these devices are properly running and linked to the network. For each network interface discovered, the *Status*, *ErrorPercent* and/or *LinkStatus* parameters are displayed:

- The *Status* parameter represents the current status of the network interface. An alert is triggered when the network interface is not responding.
- The *ErrorPercent* parameter gives the percentage of transmitted and received packets that were in error (due to low-level protocol error or physical media problems). A warning is raised when this percentage goes above 10% and an alarm when above 30%. A high error percentage often means that there is a serious problem with the cable or the interface.
- The *LinkStatus* parameter shows the current status of the network interface to the network (i.e. if it is plugged-in). By default, Hardware Sentry will trigger a warning if a network interface previously connected to the network is now unplugged. However, it will not trigger an alert for network interfaces that have never been connected.

  To change this setting, right-click the main Hardware Sentry icon and select [KM Commands] -> [Options] -> [Network link monitoring...]. This will display the dialog box shown below:


Hardware Sentry - Network link monitoring settings
Network link monitoring setting
Select how the link status of a network interface is monitored:
ALWAYS trigger an alert when a network interface is not linked to a network
NEVER trigger an alert when a network interface is not linked to a network (i.e. no monitoring of the link status)
Trigger an alert ONLY if a previously plugged-in network interface is unplugged (default)
OK
Cancel
Help

Three options are possible:

- ALWAYS trigger an alert when a network interface is not linked to a network: If a network card is unplugged, Hardware Sentry will trigger an alert no matter what.
- NEVER trigger an alert when a network interface s not linked to a network: This basically turns off the monitoring of the network link.
- Trigger an alert ONLY if the previously plugged-in network interface is unplugged: This is the default option and is explained above.

4 - Missing Device Detection

When enabled, the missing device detection mechanism of Hardware Sentry alerts the operators when a device that was previously detected in the system is no longer found.

This mechanism is very useful to alert operators when, for example, a non-redundant physical disk does not restart during a system reboot and therefore is no longer seen by the operating system and the monitoring software.

When a device is no longer discovered, its *Status* parameter goes into alarm and its label directly shows that it is missing.

5 - Connector Monitoring

When a Hardware Sentry connector has been detected as applicable to the current platform, a corresponding instance is created in the PATROL Console and its status is monitored regularly to ensure that the underlying technology is still available.

Example:

- Hardware Sentry is running on a Dell server with Dell OpenManage Server Administrator.
- Upon startup, Hardware Sentry detects Dell OpenManage Server Administrator and starts using the corresponding connector to discover the server hardware configuration and monitor the discovered devices.
- Additionally, Hardware Sentry creates an icon in the PATROL Console representing the Dell OpenManage Server Administrator connector.
- Every 2 minutes, its *Status* parameter is updated.
- If, for some reason, the Dell agent stops working, an alarm is raised on the *Status* parameter and the devices that were discovered through to this connector are taken offline.

This connector monitoring mechanism helps PATROL administrators detect hardware agent failures. It also provides a high monitoring accuracy by not confusing errors that are really encountered by devices and errors due to a monitoring tool failure.

6 - Alert Actions

Alert Actions enables the PATROL administrator to choose specific actions to be executed when a hardware failure is detected. With the Alert Actions, it is possible to:

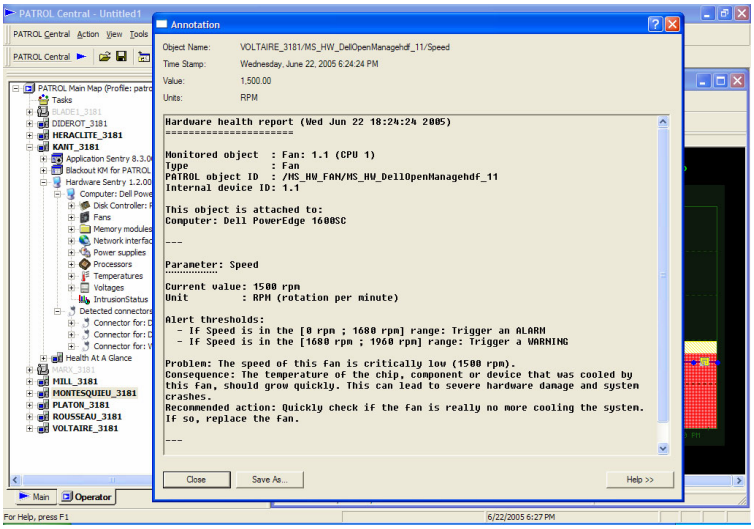
- either customize the way a hardware problem notification is performed
- or specify a recovery action to run when a problem occurs.

Alert Actions offers a large choice of actions to be executed in order to notify the operator of a problem with the hardware or to recover from a particular problem. Hardware Sentry can be configured to run one, several or all types of Alert Actions when an alert is triggered regarding the monitored hardware.

The following types of Alert Actions can be performed by Hardware Sentry:

- trigger a PATROL event
- annotate the parameter's graph
- execute an OS command
- execute a PSL command
- send a pop-up to the PATROL consoles
- write a line to a LOG file
- send a basic SNMP trap (using the PATROL MIB)
- send a custom SNMP trap

Alert Actions are highly customizable. One can customize the string that is sent through SNMP, set the username/password that is used to execute the OS Command, define the content of the PATROL event sent by Hardware Sentry, etc.


PATROL Central - Untitled1
Annotation
Object Name: VOLTAIRE_3181/MS_HW_DellOpenManagehdf_11/Speed
Time Stamp: Wednesday, June 22, 2005 6:24:24 PM
Value: 1,500.00
Units: RPM
Hardware health report (Wed Jun 22 18:24:24 2005)
Monitored object : Fan: 1.1 (CPU 1)
Type : Fan
PATROL object ID : /MS_HW_FAN/MS_HW_DellOpenManagehdf_11
Internal device ID: 1.1
This object is attached to:
Computer: Dell PowerEdge 1600SC
Parameter: Speed
Current value: 1500 rpm
Unit : RPM (rotation per minute)
Alert thresholds:
- If Speed is in the [0 rpm ; 1680 rpm] range: Trigger an ALARM
- If Speed is in the [1680 rpm ; 1960 rpm] range: Trigger a WARNING
Problem: The speed of this Fan is critically low (1500 rpm).
Consequence: The temperature of the chip, component or device that was cooled by this Fan, should grow quickly. This can lead to severe hardware damage and systen crashes.
Recommended action: Quickly check if the Fan is really no more cooling the systen. If so, replace the fan.
Close
Save As...
Help >>
Main
Operator

Additional information regarding the alert, such as the parameter name or its value, is available through the Alert Actions macros.

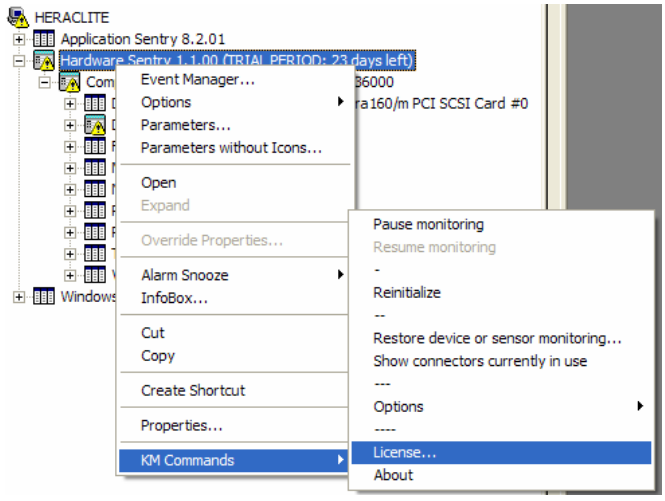
This information can be used to further customize the Alert Action triggered by Hardware Sentry and provide more details about the problem that occurs.

By default, upon hardware failure, Hardware Sentry triggers a PATROL event and annotates the parameter's graph with a comprehensive report of the problem, giving details about the failure, its possible consequences and the recommended action to solve the problem.

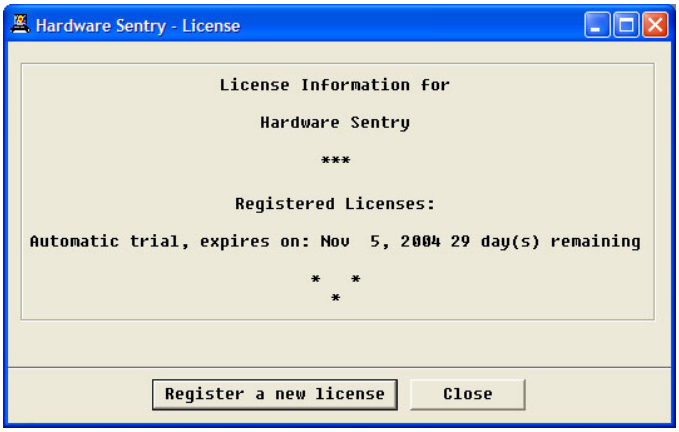
Section IV - Configuring and Administering

1 - Entering A License Key For Hardware Sentry **29**
2 - Distributing the License over Several Computers **31**
2.1 - Distributing a configuration variable with the license key *31*
2.2 - Distributing a file with the license key *31*
3 - Temporarily Suspend the Monitoring of an object **32**
4 - Terminating Monitoring of a device **33**
5 - Restoring the Monitoring of a Device after Removal **34**
6 - Choose the way Thresholds are Managed by Hardware Sentry **36**
7 - Modifying Parameter Thresholds **38**
8 - Pre-Selecting Connectors (optimizing the detection process) **40**
9 - Enabling/Disabling Missing Device Detection **42**
10 - Setting Security Options **43**
10.1 - SNMP Community *43*
10.2 - Alternate user account *43*
10.3 - Sudo Options *44*

1 - Entering A License Key For Hardware Sentry

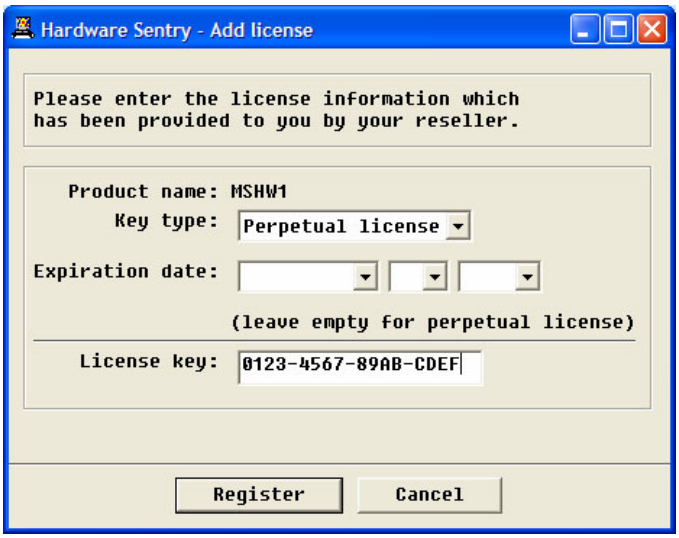


[Right-click] on the main Hardware Sentry icon > [KM Commands] > [License...]



A dialog box appears and shows the license Hardware Sentry is currently working with (automatic 30-day trial, term license or perpetual license).

To enter a new license key, click on the [Register a new license] button.

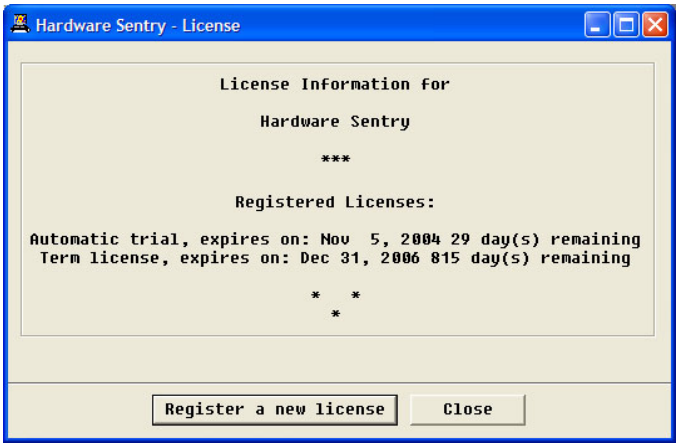

Hardware Sentry - Add license
Please enter the license information which has been provided to you by your reseller.
Product name: MSHW1
Key type: Perpetual license
Expiration date:
(leave empty for perpetual license)
License key: 0123-4567-89AB-CDEF
Register
Cancel

Choose the key type depending on the license you purchased (perpetual license or term license).

If you purchased a Term License, you have to enter your Term License expiration date.

If you purchased a Perpetual License, you should leave the expiration date field blank.

Then, enter your license key in the last field and press the [Register] button.


Hardware Sentry - License
License Information for
Hardware Sentry
***
Registered Licenses:
Automatic trial, expires on: Nov 5, 2004 29 day(s) remaining
Term license, expires on: Dec 31, 2006 815 day(s) remaining
Register a new license
Close

Once the license key has been accepted, the license dialog box is refreshed and shows the new license as registered.

Note: The automatic trial period is always shown in this dialog even if it has expired. This has no effect on the activation of Hardware Sentry.

2 - Distributing the License over Several Computers

2.1 - Distributing a configuration variable with the license key

The first way to distribute the Hardware Sentry license key to several computers is to deploy the corresponding configuration variable through wpconfig (Windows), xpconfig (Unix/Linux) or through PATROL Configuration Manager (PCM).

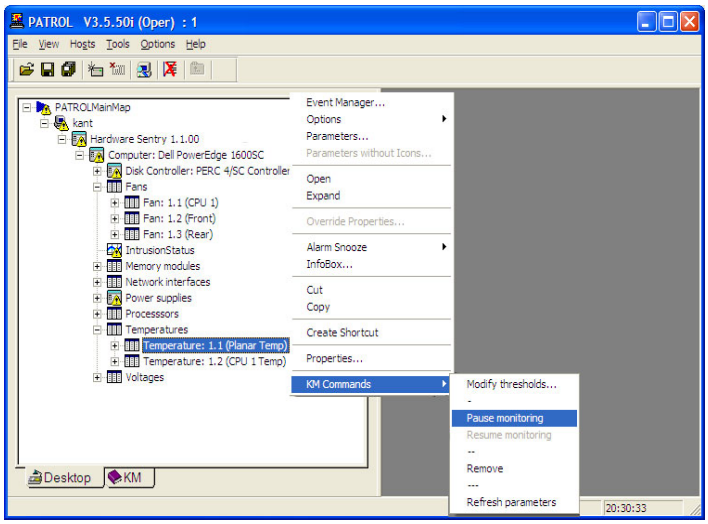
1. On a first computer, enter the license key through the graphical user interface as described in the previous section.
2. Use wpconfig, xpconfig or PATROL Configuration Manager to retrieve the /SENTRY/HARDWARE/license4 configuration variable that has been set by the graphical user interface on the first computer.
3. Distribute this /SENTRY/HARDWARE/license4 configuration variable to all of the hosts that run Hardware Sentry, through wpconfig, xpconfig or PCM.
4. The license key distributed through this mechanism will take effect within an hour.

2.2 - Distributing a file with the license key

The other way to distribute the Hardware Sentry license key to several computers is to deploy the corresponding file through any file distribution mechanism (Distribution Server, Marimba, ftp, etc.)

1. On a first computer, enter the license key through the graphical user interface as described in the previous section.
2. Retrieve the file %PATROL_HOME%\lib\MS_HW_license4 (alternatively $PATROL_HOME/lib/MS_HW_license4 under UNIX/Linux)
3. Distribute the MS_HW_license4 file to the %PATROL_HOME%\lib directory on all of the hosts that run Hardware Sentry.
4. The license key distributed through this mechanism will take effect within an hour.

3 - Temporarily Suspend the Monitoring of an object



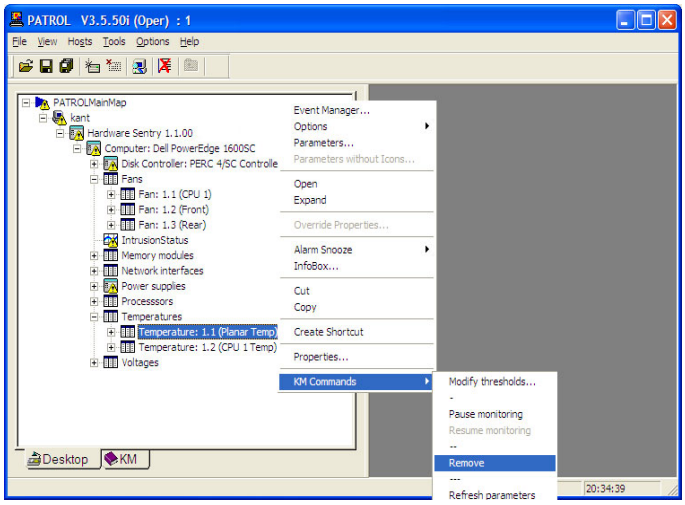
In order to perform certain tasks - maintenance for example, it may be interesting to pause the monitoring of an object by Hardware Sentry.

When in paused state, the object is still displayed in the PATROL Console but in an 'OFFLINE' status and no collect for that particular object is executed.

The monitoring of the object can simply be restarted by selecting the “Resume monitoring” option in the menu.

4 - Terminating Monitoring of a device

Information about a device may be received by Hardware Sentry through two different sources. In such a (rare) case, the monitoring of the device is performed twice and the device icon will also appear twice in the PATROL Console.

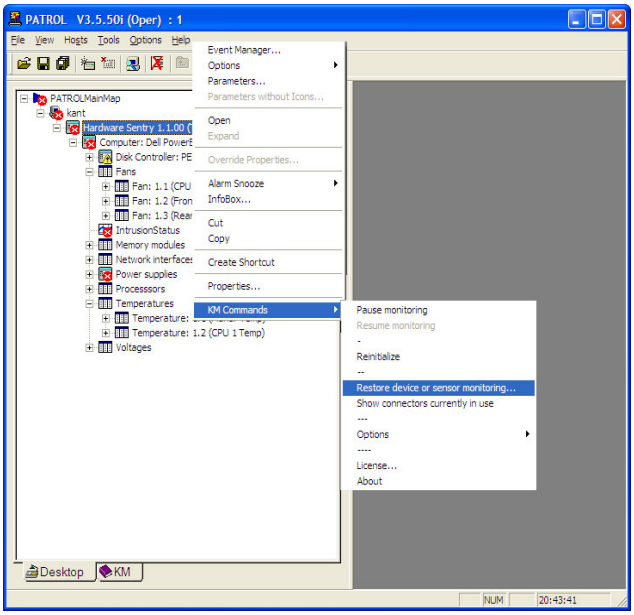


In order to avoid such redundancy, the solution is a simple: remove one of the devices monitored in the PATROL Console:

- right-click the device to remove
- select the “Remove” option from the KM Command menu

The device has been removed from monitoring which means collection for this particular device will no longer be performed, and the redundant icon representing the device will disappear from the PATROL Console.

5 - Restoring the Monitoring of a Device after Removal

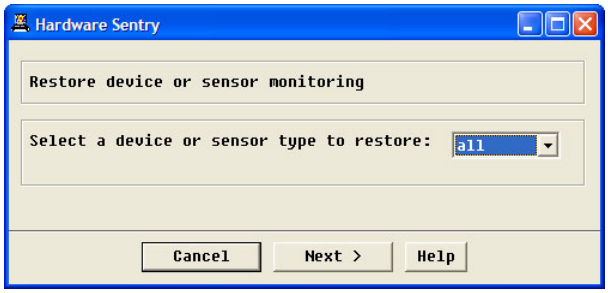


It is possible to restore device monitoring with Hardware Sentry after it has been removed from monitoring through the "Remove" option.

To check the list of the removed objects or to restore a device monitoring:

- right-click the Hardware Sentry computer icon
- select "Restore device or sensor monitoring".

If no object has been removed a message will be displayed to inform you that restoration cannot be performed. Otherwise, the first window of the Restore wizard will pop-up:



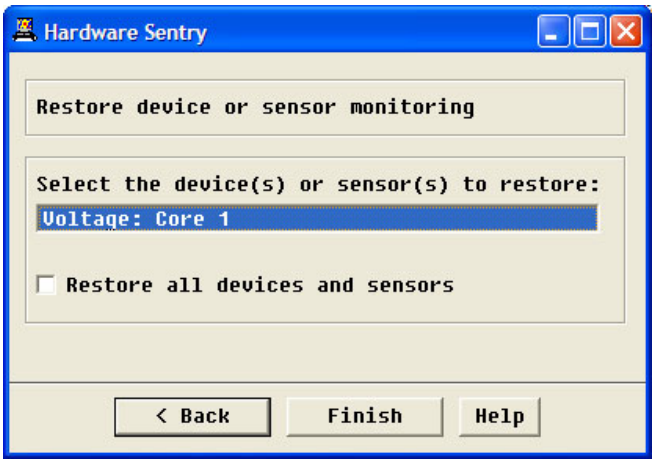
In this window, you are asked to select the type of device or sensor monitoring you would like to restore.

If, for example, you would like to restore the monitoring of a Physical Drive that you have previously removed, select "Physical disks" from the list.

If you would rather restore all monitored objects that have been removed, simply select the "All" option from the drop-down box.

Select a type and click the [Next >] button.

Note: Hardware Sentry scans the list of removed objects in order to just display the type of objects that have actually been removed. If, for instance, you have not removed any fans from monitoring, the "Fan" type will not be part of the list to choose from.



The next window shows the list of devices of the selected type that can be restored. Simply select one of several devices monitoring you would like to restore from the list and click the [Finish] button.

Checking the "Restore all devices and sensors in the list above" box will restore all devices of the selected type without selecting them one by one from the list.

Note: If you have chosen to restore "All" devices monitoring in the first window, this second window just displays the list of devices that will be restored for information.

6 - Choose the way Thresholds are Managed by Hardware Sentry

By default, Hardware Sentry automatically sets the alarm and warning thresholds on the monitored parameters. Depending on the computer it is running on, Hardware Sentry will use different thresholds for temperature parameters, voltage parameters, etc.

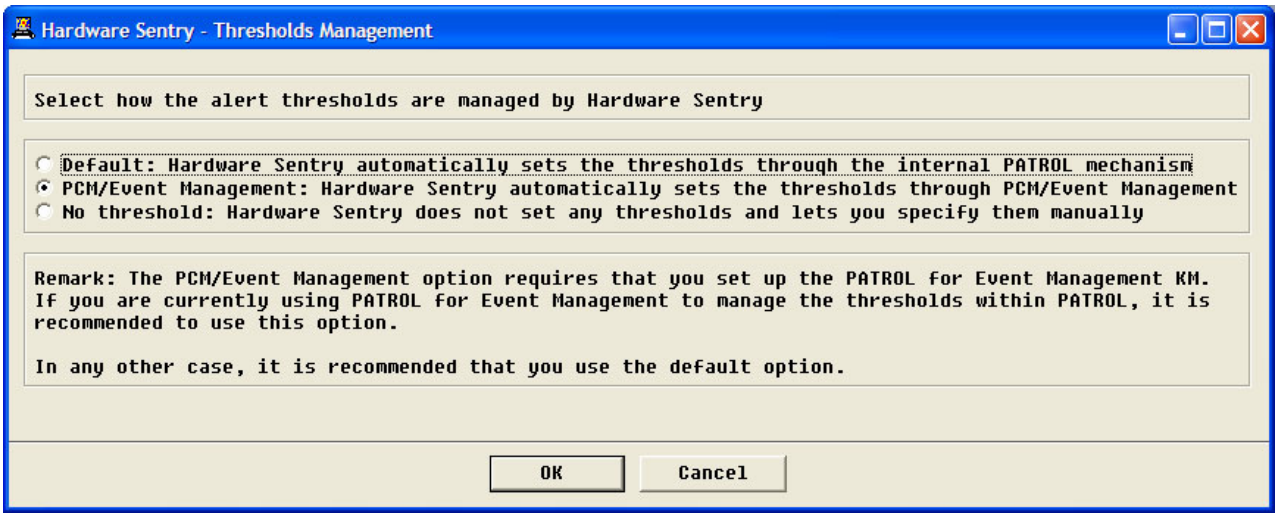
To achieve this, Hardware Sentry uses a standard internal PATROL mechanism, often known as the "Override parameters" feature. Hardware Sentry sets the alarm and warning thresholds of each parameter of each monitored object by setting a specially formatted variable under the /___tuning___ tree in the PATROL Agent configuration. This is the standard by default method to set thresholds, which is supported by BMC Software since version 3.4.11 of the PATROL Agent.

With the 3.5 release of the PATROL Agent, BMC Software started to push another way to set thresholds, which is likely to become the new thresholds standard in PATROL. This new method is known as "PATROL for Event Management" (formerly known as EventSpring) or "PATROL Configuration Manager" ("PCM", formerly known as AgentSpring). Hardware Sentry fully supports "PATROL for Event Management" and is able to manage its thresholds through this new mechanism.

By default, Hardware Sentry uses the "Override parameters" mechanism to manage its thresholds because it is the only one which does not require any additional piece of software to run on the managed computer.

To make Hardware Sentry uses the "PATROL for Event Management" mechanism for its thresholds, [right-click] on the main Hardware Sentry icon, [KM Commands] > [Options] > [Thresholds management...].

The following dialog box appears:


Hardware Sentry - Thresholds Management
Select how the alert thresholds are managed by Hardware Sentry
Default: Hardware Sentry automatically sets the thresholds through the internal PATROL mechanism
PCM/Event Management: Hardware Sentry automatically sets the thresholds through PCM/Event Management
No threshold: Hardware Sentry does not set any thresholds and lets you specify them manually
Remark: The PCM/Event Management option requires that you set up the PATROL for Event Management KM.
If you are currently using PATROL for Event Management to manage the thresholds within PATROL, it is recommended to use this option.
In any other case, it is recommended that you use the default option.
OK
Cancel

You can select one of the three following options:

- "Default": Hardware Sentry will manage its thresholds through the standard "Override parameters" mechanism. Thresholds are stored in the PATROL Agent configuration under the /___tuning___ tree. This option is set by default and does not require any additional software. If you do not use PATROL for Event Management, it is strongly recommended that you use this option.

- "PCM/Event Management": Hardware Sentry will manage its thresholds through the PCM or Event Management mechanism. Thresholds are stored in the PATROL Agent configuration under the /AS tree. This option requires that you set up the PATROL for Event Management KM on your PATROL Agent. PATROL for Event Management has to be enabled and preloaded. If you already use PATROL for Event Management in order to modify or customize your thresholds, it is strongly recommended that you use this option.
- No threshold: Hardware Sentry will not set any threshold on its monitored objects and lets you specify the thresholds through your preferred method.

  Warning! In order to avoid side effects and unpredictable behavior, if you select the default or the "PCM/Event Management" thresholds management option, Hardware Sentry will automatically remove the thresholds set through the other method (only for its monitored objects). That is: if you select the "PCM/Event Management" option, Hardware Sentry will automatically remove all the thresholds (set for its monitored objects) stored in the /___tuning___ tree in the PATROL Agent configuration.

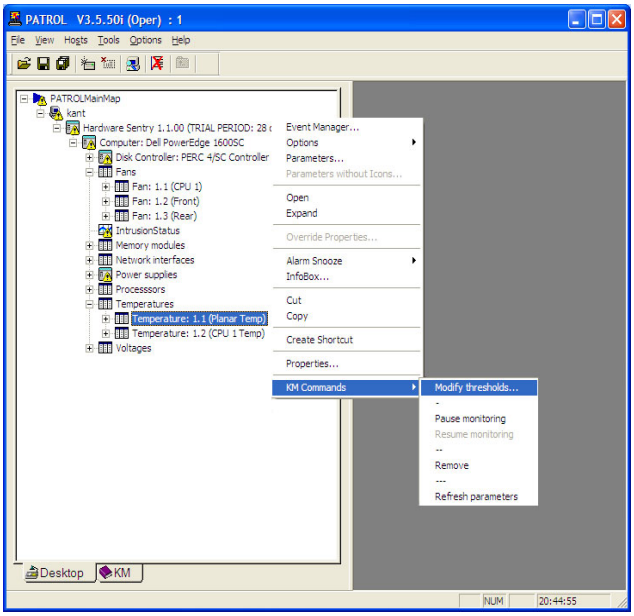
  Note: Hardware Sentry is fully compatible with the PCM/Event Management thresholds management mechanism. All the classes are provided with no threshold set.

  Note: the "default" and "PCM/Event Management" thresholds management options still imply that Hardware Sentry automatically sets these thresholds during its discovery. In other words, if you use the "Override parameter" interface in the PATROL Console or the "PATROL for Event Management" interface to manually set thresholds on the Hardware Sentry parameters, they will be quickly (less than one hour) overwritten by the discovery process.

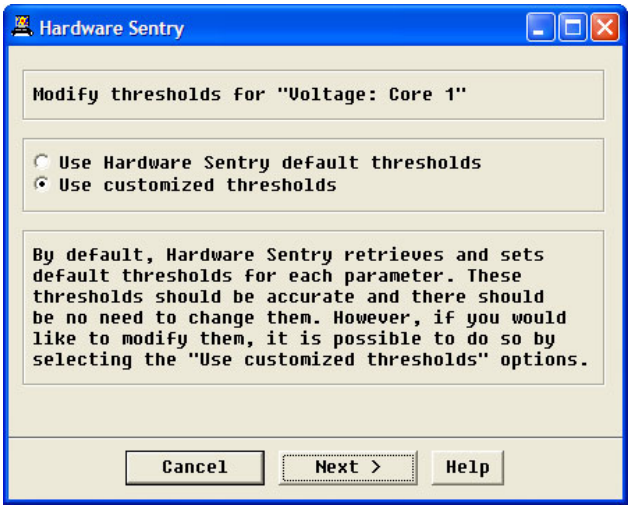
  For details on how to manually set thresholds on the Hardware Sentry parameters, please see the next section.

7 - Modifying Parameter Thresholds

Whenever possible, Hardware Sentry automatically sets thresholds for parameters. These thresholds are retrieved from available information and they are generally accurate. Normally, there is no need to modify these thresholds but in case Hardware Sentry cannot obtain them, or if prefer a more fault-tolerant monitoring, you can modify the thresholds of each parameter through the command menu.



To do so, right-click on the device monitoring (but not directly on the parameter) and select "Modify Thresholds"


Hardware Sentry
Modify thresholds for "Voltage: Core 1"
Use Hardware Sentry default thresholds
Use customized thresholds
By default, Hardware Sentry retrieves and sets default thresholds for each parameter. These thresholds should be accurate and there should be no need to change them. However, if you would like to modify them, it is possible to do so by selecting the "Use customized thresholds" options.
Cancel
Next >
Help

The first panel of the "Modify thresholds" explains the purpose of this option.

Here you are asked to choose between letting Hardware Sentry use the default values or modifying them and setting your own thresholds.

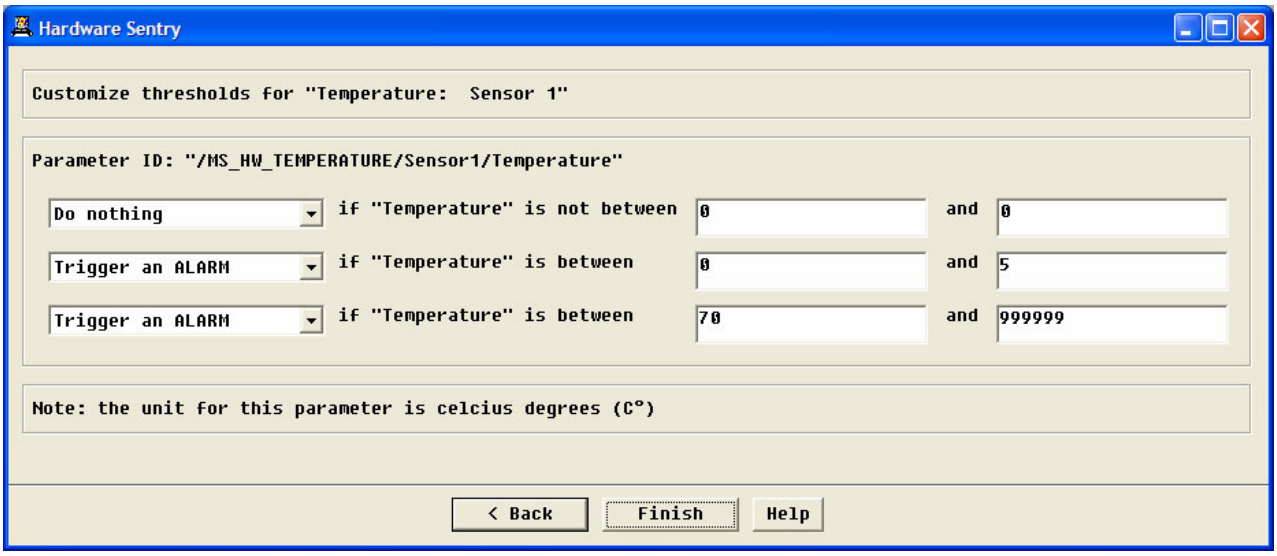
If you select the first option "Use Hardware Sentry default values", which is the recommended one, and click the [Next] button, the next panel will display information about the parameter thresholds. There is no choice to make in this panel besides confirming the use of default thresholds by clicking the [Finish] button.

Clicking on [Back] brings you back to the first window where you can modify your choice and select the "Use customized thresholds" option.

This option brings you to a different panel where you are asked to enter new thresholds for the parameter. Setting them up is easy, as you enter thresholds as if you were making a sentence.

On the left side, the drop-down box is used to select the severity of the event triggered when one of the thresholds is reached: none (“Do nothing”), warning or an alert.

The purpose of the right side of the panel is to enter the thresholds themselves.



Note: If you have selected the default thresholds management option (see previous section), your customized thresholds are stored under the /___tuning___ tree in the PATROL Agent configuration and then can be modified through the "Override parameter" feature of the PATROL Console.

If you have selected the "PCM/Event Management" thresholds management option, your customized thresholds are stored under the /AS tree in the PATROL Agent configuration and then can be modified through the "PATROL for Event Management" (EventSpring) interface or through the "PATROL Configuration Manager" graphical user interface.

If you have selected the "no threshold" option, your customized thresholds simply will not be stored.

8 - Pre-Selecting Connectors (optimizing the detection process)

Hardware Sentry's detection process may take some time depending on the platform. Although it is only done upon the PATROL Agent startup, if performance is an issue it might be wise to speed things up by pre-selecting the platforms to be used to monitor.

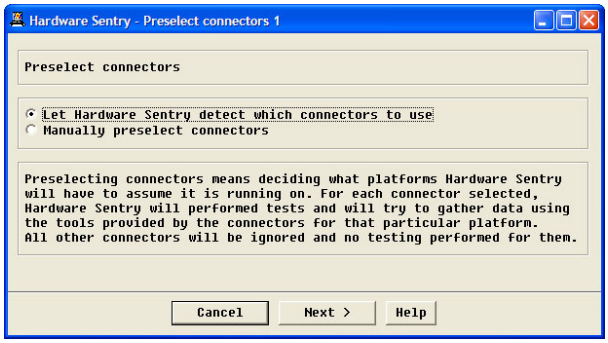
Pre-selecting connectors means that an administrator decides what platforms Hardware Sentry will have to assume it is running on. For each connector selected, Hardware Sentry will perform tests and will try to gather data using the tools provided by the connectors for that particular platform. All other connectors (and therefore other platforms) will be ignored and no testing shall be performed for them.

The downside of pre-selection is that if the wrong connectors are selected, then no monitoring will be performed. Furthermore, if some hardware that does not belong to the pre-selected platforms is added to the server later on, it won't be detected.

It is therefore strongly recommended to let Hardware Sentry figure out what type of platforms can be found on the system and the pre-selection option should be used by advanced users only.

To pre-select connectors, right-click the main Hardware Sentry icon and select the "Pre-select connectors" in the "Options" menu.

The following dialog box is displayed:


Hardware Sentry - Preselect connectors 1
Preselect connectors
Let Hardware Sentry detect which connectors to use
Manually preselect connectors
Preselecting connectors means deciding what platforms Hardware Sentry will have to assume it is running on. For each connector selected, Hardware Sentry will performed tests and will try to gather data using the tools provided by the connectors for that particular platform. All other connectors will be ignored and no testing performed for them.
Cancel
Next >
Help

Two choices are possible in this window:

- Let Hardware Sentry detect which connectors to use: in this mode, Hardware Sentry will run tests at each discovery and select the connectors that match the current system.
- Manually pre-select connectors: selecting this option lets you decide which connectors Hardware Sentry should use to monitor the system Hardware.

Note: when the panel comes up, the selected option is the one that is currently in use.

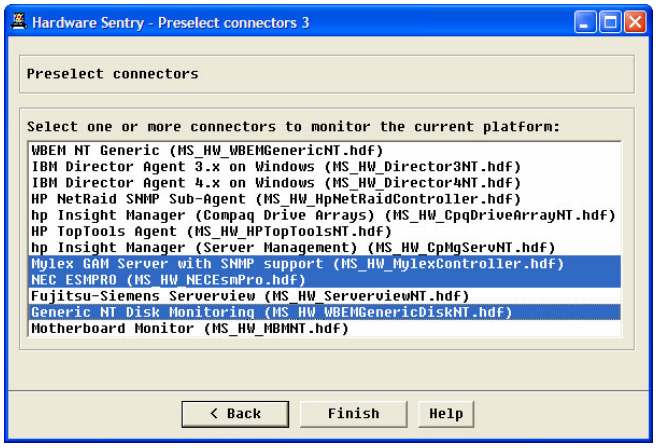
The first option, "Let Hardware Sentry detect which connectors to use" is the recommended one and the one used by default when Hardware Sentry is loaded on a PATROL Agent. The detection process is very efficient and accurate, and should not use the computer's resources extensively. If this option is selected, clicking on the [Next] button will bring up a panel with a message saying Hardware Sentry will run the detection process again.

If the manual pre-selection is chosen, the [Next] panel displays a list of connectors to choose from.

It is possible to select several connectors from the list by simply clicking on them. Unselecting a connector is also performed by clicking on its item on the list.

Each item contains the display name of the connector as well as its corresponding file name on the system. The list is built from the content of the directory: "%PATROL_HOME%/lib/MS_HW_HDF"

Once the selection is made, click the [Finish] button to let Hardware Sentry re-run a detection process with the new connector selection.


Hardware Sentry - Preselect connectors 3
Preselect connectors
Select one or more connectors to monitor the current platform:
WBEM NT Generic (MS_HW_WBEMGenericNT.hdf)
IBM Director Agent 3.x on Windows (MS_HW_Director3NT.hdf)
IBM Director Agent 4.x on Windows (MS_HW_Director4NT.hdf)
HP NetRaid SNMP Sub-Agent (MS_HW_HpNetRaidController.hdf)
hp Insight Manager (Compaq Drive Arrays) (MS_HW_CpqDriveArrayNT.hdf)
HP TopTools Agent (MS_HW_HPTopToolsNT.hdf)
hp Insight Manager (Server Management) (MS_HW_CpMgServNT.hdf)
Mylex GAM Server with SNMP support (MS_HW_MylexController.hdf)
NEC ESMPRO (MS_HW_NECEsmPro.hdf)
Fujitsu-Siemens Serverview (MS_HW_ServerviewNT.hdf)
Generic NT Disk Monitoring (MS_HW_WBEMGenericDiskNT.hdf)
Motherboard Monitor (MS_HW_MBMNT.hdf)
< Back
Finish
Help

Note: At the end of the Pre-selection wizard, Hardware Sentry will run a full discovery. All devices and sensors will be re-detected. If the connector list differs from what Hardware Sentry was using previously, new devices monitored may appear in the PATROL Console and old ones may be removed. If this is the case, pay close attention to the PATROL System Output Window for error messages. A bad selection of connectors may remove all devices and sensors and may prevent Hardware Sentry from being able to monitor the system's hardware!

9 - Enabling/Disabling Missing Device Detection

Hardware Sentry can detect missing devices in the system. If at one point, information about a device that was previously being monitored cannot be obtained anymore, the device is considered missing. In this case, an alert is triggered and the missing status of the device is added to its label.

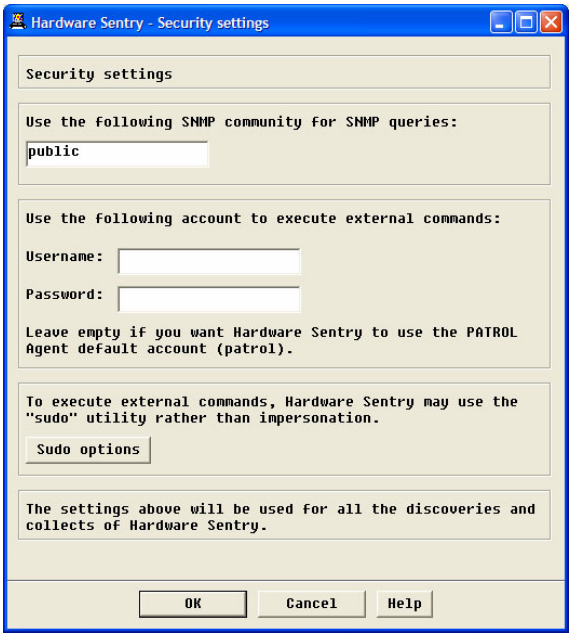
Hardware Sentry - Missing device detection
Missing device detection
Disable missing device detection
By default, Hardware Sentry monitors and detects missing devices, i.e. devices that may disappear during the monitoring or after a reboot.
OK
Cancel

The missing device detection works for all the devices discovered by Hardware Sentry.

It is enabled by default and can be disabled through a KM Command: [right-click] on the main Hardware Sentry icon > [Options] > [Missing device toggle...].

Note: Disabling this option when some missing devices have already been detected will simply remove these devices from monitoring.

10 - Setting Security Options


Hardware Sentry - Security settings
Security settings
Use the following SNMP community for SNMP queries:
public
Use the following account to execute external commands:
Username:
Password:
Leave empty if you want Hardware Sentry to use the PATROL Agent default account (patrol).
To execute external commands, Hardware Sentry may use the "sudo" utility rather than impersonation.
Sudo options
The settings above will be used for all the discoveries and collects of Hardware Sentry.
OK
Cancel
Help

To access the "Security settings" dialog, [right-click] the main Hardware Sentry icon (computer), [KM Commands] > [Options] > [Security Settings...].

10.1 - SNMP Community

Hardware Sentry allows you to modify the SNMP community that will be used for SNMP queries.

In the Security Settings dialog, enter the custom SNMP community in the first field. Leave this field blank if you want Hardware Sentry to automatically decide which SNMP community string to use.

Using an alternate SNMP community can be required in secured network environments where all the SNMP agents are configured in a customized community.

10.2 - Alternate user account

Using an alternate account (different from the PATROL default account) to execute external commands (OS commands and WBEM queries) is needed in secured systems where the PATROL Agent default account does not have all the privileges required in order to perform queries against some hardware devices.

This is also true for HP-UX systems (to access physical disks) as well as IBM xSeries computers under Linux (to make WBEM requests). Please refer to the Hardware Sentry Installation Guide for more information specific to these platforms.

In the Security Settings dialog, enter the username/password to be used to execute eternal commands. Leave these fields empty if you want Hardware Sentry to use the PATROL Agent default account.

Note: In order to take effect, these settings need the agent to be restarted.

10.3 - Sudo Options

Depending on the targeted platform, Hardware Sentry may use some external system utilities to gather hardware information. Sometimes the PATROL Agent default account does not have sufficient privileges to execute these commands and it is not possible in your environment to give super-user rights to the PATROL Agent (as described above).

In such case Hardware Sentry uses the “sudo” utility to execute external commands as “root”. The “sudo” utility helps UNIX system administrators secure their environment by authorizing some users to execute only some specified commands as another user account (typically root).

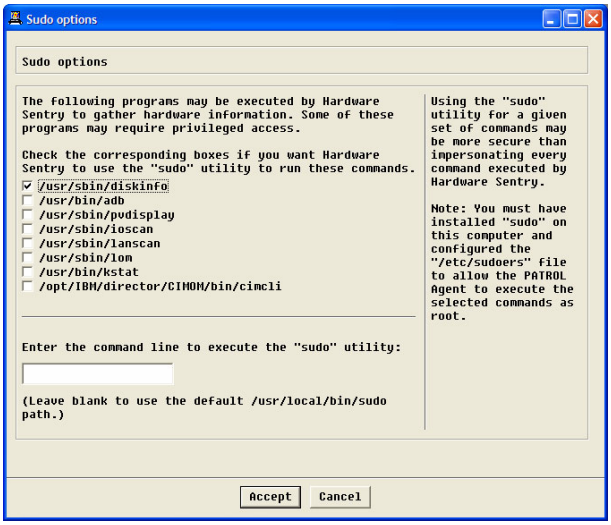
If the case described above applies to you, the “sudo” options may be a good workaround. Here is the procedure to configure Hardware Sentry to use “sudo”:

1. Identify which commands that are run by Hardware Sentry needs advanced privileges.

   - /usr/sbin/diskinfo on HP-UX systems

   - /opt/IBM/director/CIMOM/bin/cimcli on IBM xSeries systems under Linux

2. Configure “sudo” to allow the PATROL Agent default account to execute the needed commands as root (modify the /etc/sudoers file). Configuring “sudo” requires root privileges.
3. Check that the PATROL Agent default account is properly authorized to execute needed commands through the “sudo” utility.
4. Ensure that the “sudo” bin directory is in the PATH variable of the PATROL environment.
5. Go to the Hardware Sentry “Security Settings” dialog in the PATROL Console and click on the “Sudo options” button.
6. Check the boxes corresponding to the commands that have been configured in “sudo”.
7. Restart the PATROL Agent

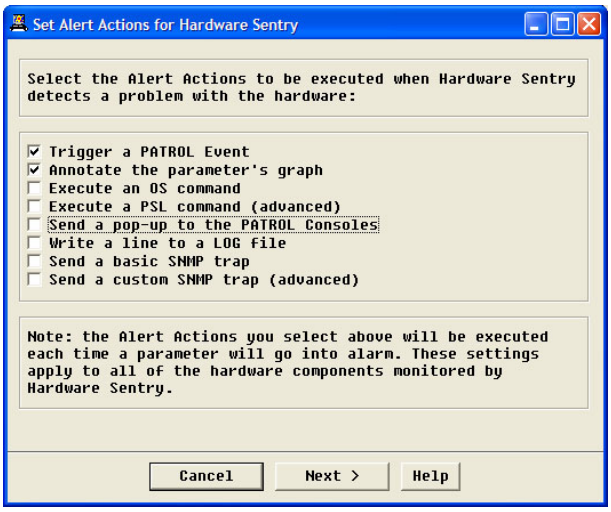

Sudo options
Sudo options
The following programs may be executed by Hardware Sentry to gather hardware information. Some of these programs may require privileged access.
Check the corresponding boxes if you want Hardware Sentry to use the "sudo" utility to run these commands.
/usr/sbin/diskinfo
/usr/bin/adb
/usr/sbin/pvdisplay
/usr/sbin/ioscan
/usr/sbin/lanscan
/usr/sbin/lom
/usr/bin/kstat
/opt/IBM/director/CIMOM/bin/cimcli
Using the "sudo" utility for a given set of commands may be more secure than impersonating every command executed by Hardware Sentry.
Note: You must have installed "sudo" on this computer and configured the "/etc/sudoers" file to allow the PATROL Agent to execute the selected commands as root.
Enter the command line to execute the "sudo" utility:
(Leave blank to use the default /usr/local/bin/sudo path.)
Accept
Cancel

Note: This option is available on UNIX and Linux platforms only.

11 - Editing Alert Actions

To modify the Alert Actions executed by Hardware Sentry upon a hardware failure, [right-click] on the main Hardware Sentry icon > [KM Commands] > [Options] > [Edit Alert Actions…]

11.1 - Select the Alert Actions to be executed


Set Alert Actions for Hardware Sentry
Select the Alert Actions to be executed when Hardware Sentry detects a problem with the hardware:
Trigger a PATROL Event
Annotate the parameter's graph
Execute an OS command
Execute a PSL command (advanced)
Send a pop-up to the PATROL Consoles
Write a line to a LOG file
Send a basic SNMP trap
Send a custom SNMP trap (advanced)
Note: the Alert Actions you select above will be executed each time a parameter will go into alarm. These settings apply to all of the hardware components monitored by Hardware Sentry.
Cancel
Next >
Help

Check the boxes corresponding to the actions you would like executed upon a hardware failure.

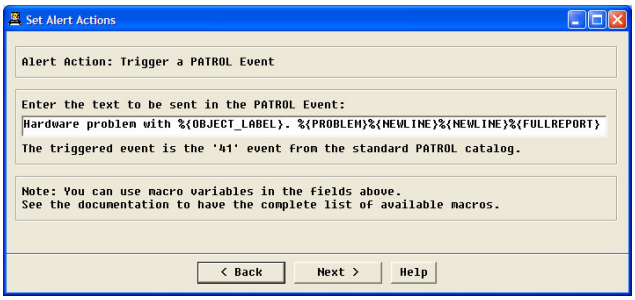
By default, Hardware Sentry triggers a PATROL event and annotates the parameter that raises the alert.

11.2 - Trigger a PATROL Event

If you have selected the “Trigger a PATROL Event” action, you need to enter the string that will be displayed with the event.

A PATROL Event can be viewed from:

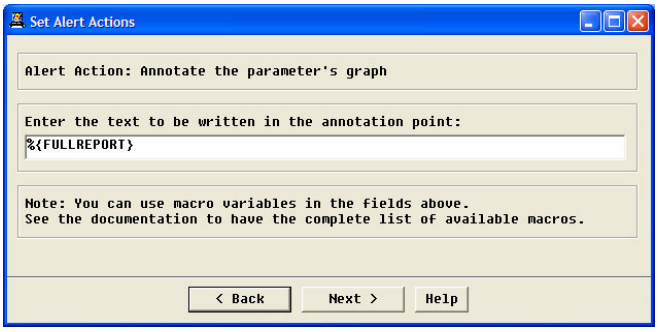
- Standard PATROL Consoles (Classic Console, PATROL Central)
- PATROL Enterprise Manager
- BMC Impact Manager
- Other third-party products that interface with PATROL.


Set Alert Actions
Alert Action: Trigger a PATROL Event
Enter the text to be sent in the PATROL Event:
Hardware problem with %{OBJECT_LABEL}. %{PROBLEM}%{NEWLINE}%{NEWLINE}%{FULLREPORT}
The triggered event is the '41' event from the standard PATROL catalog.
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

Note: The PATROL event that is triggered is the ‘41’ event from the standard PATROL catalog.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

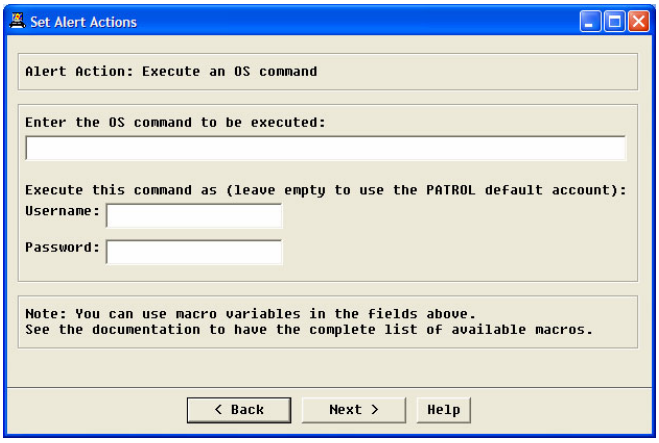
11.3 - Annotate the Parameter's Graph


Set Alert Actions
Alert Action: Annotate the parameter's graph
Enter the text to be written in the annotation point:
%{FULLREPORT}
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

If you select the "Annotate the parameter's graph" action, you need to enter the string that will be displayed within the annotation point.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

11.4 - Execute an OS command


Set Alert Actions
Alert Action: Execute an OS command
Enter the OS command to be executed:
Execute this command as (leave empty to use the PATROL default account):
Username:
Password:
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

If you select the "Execute an OS command" action, you need to enter:

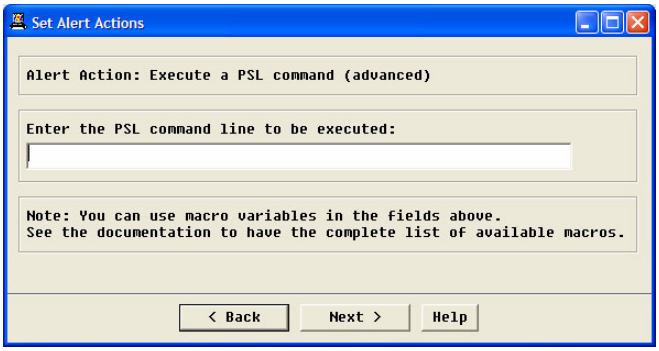
- command line to be executed
- user and password used to run the command.

The command can be a program utility or a script shell, and can have arguments.

Warning! The command must be non-interactive (no window, no user input).

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

11.5 - Execute a PSL command

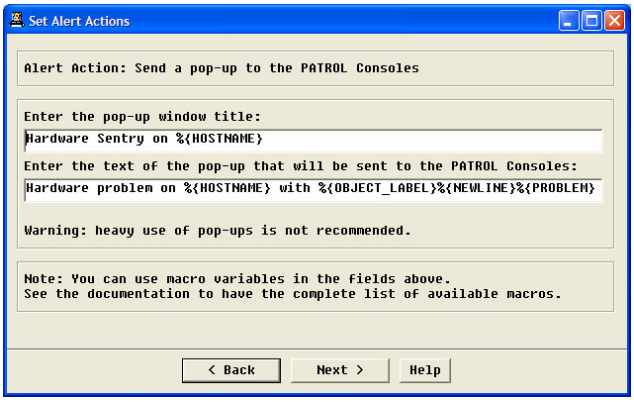

Set Alert Actions
Alert Action: Execute a PSL command (advanced)
Enter the PSL command line to be executed:
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

If you select the "Execute a PSL command" action, you need to enter the PSL statement to be executed by the PATROL Agent. Only a single line is permitted but it can have several PSL instructions.

Warning! The PSL command is recommended for PATROL advanced users only.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

11.6 - Send a Pop-up to the PATROL Consoles


Set Alert Actions
Alert Action: Send a pop-up to the PATROL Consoles
Enter the pop-up window title:
Hardware Sentry on %{HOSTNAME}
Enter the text of the pop-up that will be sent to the PATROL Consoles:
Hardware problem on %{HOSTNAME} with %{OBJECT_LABEL}%{NEWLINE}%{PROBLEM}
Warning: heavy use of pop-ups is not recommended.
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

If you select the "Send a pop-up to the PATROL Consoles" action, you need to enter the message that will be displayed in the pop-up as well as the title of the pop-up window.

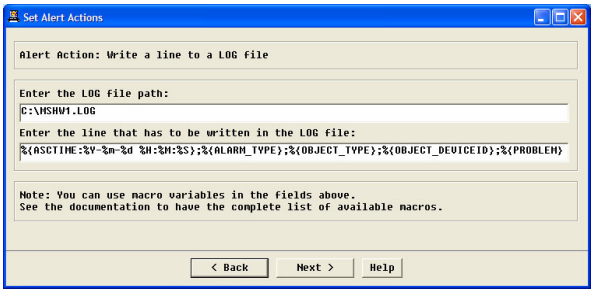
Warning! Too many pop-ups could annoy the operators.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

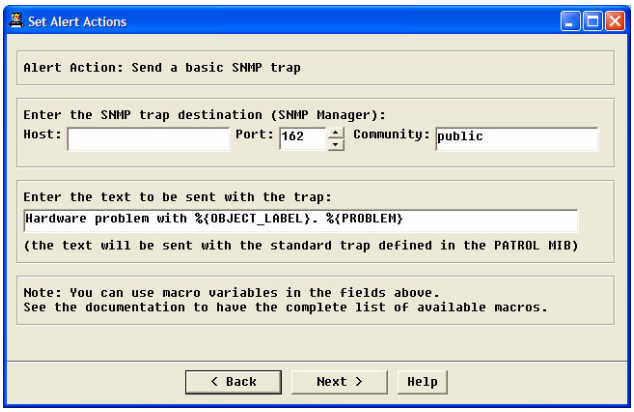
11.7 - Write a line to a LOG file

If you select the "Write a line to a LOG file" action, you need to enter the LOG file path where Hardware Sentry will write a line, as well as the content of the line to be written.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.


Set Alert Actions
Alert Action: Write a line to a LOG file
Enter the LOG file path:
C:\MSHW1.LOG
Enter the line that has to be written in the LOG file:
%{ASCTIME:%Y-%m-%d %H:%M:%S};%{ALARM_TYPE};%{OBJECT_TYPE};%{OBJECT_DEVICEID};%{PROBLEM}
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

11.8 - Send a Basic SNMP trap


Set Alert Actions
Alert Action: Send a basic SNMP trap
Enter the SNMP trap destination (SNMP Manager):
Host:
Port: 162
Community: public
Enter the text to be sent with the trap:
Hardware problem with %{OBJECT_LABEL}. %{PROBLEM}
(the text will be sent with the standard trap defined in the PATROL MIB)
Note: You can use macro variables in the fields above.
See the documentation to have the complete list of available macros.
< Back
Next >
Help

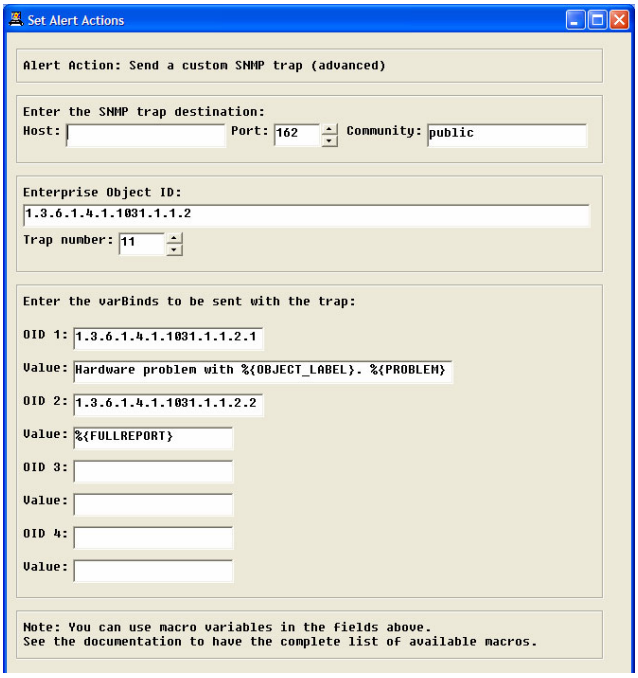
If you select the "Send a basic SNMP trap" action, you need to enter:

- The IP address or hostname of the SNMP manager that the trap will be issued to
- The SNMP community string used by the SNMP manager.
- The text that will be sent in the SNMP trap.

Note: Upon a hardware failure, Hardware Sentry will send the trap that is defined in the PATROL MIB (Trap number 11, Enterprise ID: 1.3.6.1.4.1.1031.1.1.2, the text is stored in the 1.3.6.1.4.1.1031.1.1.2.1 OID).

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

11.9 - Send a custom SNMP trap (advanced)



If you select the "Send a custom SNMP trap" action, you need to enter the following:

- The IP address or hostname of the SNMP manager that the trap will be issued to.
- The SNMP community string used by the SNMP manager
- All the characteristics of the trap: Enterprise ID, trap specific number and up to 4 varbinds.

Note: You can use macros that will be replaced at runtime. The list of available macros is described later in this chapter.

11.10 - Macro Variables

Macro variables can be used in the Alert Actions to customize a string with information related to the encountered hardware failure (display name of the faulty object, value of the parameter, description of the problem, etc.)

Example: You can configure Hardware Sentry to trigger a PATROL event containing the display name of the faulty object by entering something like "*Hardware problem with %{OBJECT_NAME}*" in the "Trigger a PATROL Event" dialog box.

Note: You can use several macros at one time.

The table below recapitulates the available macros in the Alert Actions.

Macro	Description
%{PARAMETER_NAME}	Name of the parameter that triggered the alert Example: PredictedFailure
%{VALUE}	Formatted value (with unit) of the parameter that triggered the alert Example: 67.3 °C
%{RAW_VALUE}	Raw value of the parameter that triggered the alert Example: 67.30000
%{ALARM_TYPE}	Alarm type (INFORMATION, WARNING or ALARM) Example: ALARM
%{PROBLEM}	Description of the problem encountered by the monitored device Example: The speed of this fan is critically low (1503 rpm).
%{CONSEQUENCE}	Description of the possible consequence of the detected problem Example: The temperature of the chip, component or device that was cooled by this fan should grow quickly. This can lead to severe hardware damage and system crashes.
%{RECOMMENDED_ACTION}	Recommended action to solve the problem Example: Quickly check if the fan is really no more cooling the system. If so, replace the fan.
%{OBJECT_ID}	PATROL internal ID of the instance that triggered the alert Example: MS_HW_DellOpenManagehdf_11

Macro	Description
%{OBJECT_LABEL}	Display name of the instance that triggered the alert Example: Fan: 1.1 (CPU 1)
%{OBJECT_CLASS}	Class of the instance that triggered the alert Example: MS_HW_FAN
%{OBJECT_TYPE}	Type of the device that triggered the alert Example: Fan
%{OBJECT_DEVICEID}	Hardware Sentry internal device ID of the instance that triggered the alert Example: 1.1
%{PARENT_ID}	PATROL internal ID of the object that the faulty instance is attached to Example: MS_HW_DellOpenManagehdf_1
%{PARENT_LABEL}	Display name of the object that the faulty instance is attached to Example: Computer: Dell PowerEdge 1600SC
%{PARENT_CLASS}	Class of the object that the faulty instance is attached to Example: MS_HW_ENCLOSURE
%{PARENT_TYPE}	Type of the object that the faulty instance is attached to Example: Computer enclosure
%{PARENT_DEVICEID}	Hardware Sentry internal device ID of the object that the faulty instance is attached to Example: 1
%{HOSTNAME}	Host name of the computer that the PATROL Agent is running on Example: SENTRYTEST003
%{DATE}	Current date in the YYYY-MM-dd format Example: 2005-6-23
%{TIME}	Current time in the HH:MM:SS format Example: 11:14:53
%{ASCTIME:…}	Current date and time formatted as specified in the macro Example: %{ASCTIME:%m %d %T %Y} will produce Jun 6 11:14:53 2005 The available formats for the %{ASCTIME:…} macro are listed in the asctime() description of the PSL Reference Guide (Book 2).
%{/variable_name}	Value of the *variable_name* instance variable Example: %{/worstParam} will give the name of the “worst parameter” of the instance that triggered the alert. This feature is recommended for advanced users only!
%{NEWLINE} %{\n}	Linefeed. This is useful to produce multi-line information.
%{FULLREPORT}	Full hardware health report about the instance that triggered the alert Example: see the output of the “Show hardware health report” Menu command

Section V - Inside Hardware Sentry

1 - Architecture 51
2 - The .HDF files (connectors) 52
3 - The Detection Process 53
4 - The Discovery Process 54
5 - The Collection Process 55

1 - Architecture

As described in the first chapter ("Getting Started"), Hardware Sentry KM for PATROL is mainly composed of:

- a common hardware monitoring engine (MS_HW_*.km KM classes and ms_hw_*.lib PSL libraries that run with the PATROL Agent of each monitored computer)
- several connector files (MS_HW_*.hdf) that are platform-specific.

Upon startup, Hardware Sentry tests each connector in order to detect which hardware information sources are available (vendor-specific hardware agents, standards instrumentation layers, etc.). This is called the "detection process".

Once Hardware Sentry knows which hardware information sources are available and can be connected to, it tries to discover the hardware environment by querying these selected hardware information sources, as described in the corresponding *.hdf files. This is called the "discovery process".

Finally, when the detection and discovery processes are complete, Hardware Sentry starts collecting data about the discovered hardware environment (status, temperatures, voltages, etc.) by querying the detected hardware information sources as described in the corresponding *.hdf files. This is called the "collection process".

The table below shows the synopsis of the actions performed by Hardware Sentry.

Action	Job done	Corresponding PATROL process
Activation	Activates the MS_HW_MAIN class.	PRE-DISCOVERY process of the MS_HW_MAIN class. Executed once on the PATROL Agent startup.
License check	Creates the MS_HW_MAIN icon. Look for a valid license key. Activates all of the Hardware Sentry classes.	DISCOVERY process of the MS_HW_MAIN class. Executed every hour (default period).
Detection Process	Tests each connector in order to detect which hardware information sources are available and can be connected to.	
Discovery Process	Discovers the hardware environment by querying the previously detected hardware information sources. Creates the other class instances (MS_HW_TEMPERATURE, MS_HW_PHYSICALDISK, etc.)	
Collection Process	Polls previously detected hardware information sources to gather data about the hardware environment.	Collector parameters of the MS_HW_MAIN class: fanColl, logicalDiskColl, otherDeviceColl, etc. Executed every 2nd minute (default period).

2 - The .HDF files (connectors)

Each connector is an ".hdf" file that is dedicated to one hardware information source. The purpose of each ".hdf" file is to describe how Hardware Sentry can connect to the hardware information source available on a platform and which information is available through this source. For example, MS_HW_Director41NT.hdf will describe how to get information from the IBM Director 4.1 Agent and then monitor an IBM xSeries server.

A ".hdf" file can tell the Hardware Sentry engine to do the following actions:

- query a SNMP agent (get, get_next, and tables)
- execute a WBEM query
- execute an OS command

Each ".hdf" file uses a mix of these possible actions with some computing capabilities to make Hardware Sentry gather useful data in a given hardware information source.

Note: The ".hdf" files are located under the "`MS_HW_hdf`" folder under "`%PATROL_HOME%/lib`". All ".hdf" files are installed on all platforms.

Note: The ".hdf" files released by Sentry Software are encrypted and therefore cannot be updated or modified by the end-user.

Note: The whole HDF syntax will be described in a separate document and will allow users to write their own ".hdf" files. Hardware Sentry will work with custom ".hdf" files as it works with officially released one.

3 - The Detection Process

As Hardware Sentry KM for PATROL is preloaded by the PATROL Agent, it begins its operations upon the agent startup. Once the Hardware Sentry pre-discovery PSL process has activated the MS_HW_MAIN class, the PATROL Agent spawns the Hardware Sentry discovery PSL process. This PSL process takes two actions: the detection and the environment discovery. Here is a description of this detection process.

- Get the list of available connectors ("*.hdf" files in the `%PATROL_HOME%/lib/MS_HW_hdf` folder)
- For each ".hdf" file found, test the detection criteria (OS type, NT service, processes, SNMP request, etc.)
- Mark the ".hdf" files as "detected" once all its detection criteria is successfully passed. There may be several connectors detected at one time (typically: one connector for the temperatures, voltages, etc., one for the RAID disk controller and one for the non-RAID disk controller).
- Launch the discovery process.

Note: only one ".hdf" file can describe the computer model and manufacturer, as only one icon for the computer will be created. The Hardware Sentry engine will ensure that only one ".hdf" describing the computer model will be marked as "detected".

Note: to optimize the detection process and gain some time, the detection process is heavily parallelized. All the ".hdf" files are processed simultaneously.

4 - The Discovery Process

The discovery process is launched just after the end of the detection process. It takes the following actions:

- Processes the "Enclosure.Discovery" section of the detected connectors (“.hdf”) that describe the computer model and create the main Hardware Sentry and computer icon (class: MS_HW_ENCLOSURE). Most of other icons (disk controllers, fans, temperatures, etc.) will be created under this computer icon.
- Launches the disk controller discovery that will processes the "DiskController.Discovery" section of each detected “.hdf” file and create the MS_HW_DISKCONTROLLER icons.
- Launches the other discoveries (fans, temperatures, voltages, power supplies, logical disks, physical disks and other devices) that will process the corresponding sections of each detected “.hdf” file and create the corresponding icons.

Note: With a view to optimization, the discovery process is as parallelized as possible. All the independent objects are processed at the same time.

5 - The Collection Process

Once the discovery process is complete, the collection process starts. Every two minutes, Hardware Sentry spawns several PSL processes (fanColl, physicalDiskColl, logicalDiskColl, temperatureColl, etc.) that are responsible for the collection of information about a given device type. For example, fanColl will gather fan information from the different detected hardware information sources, as described in the corresponding ".hdf" Fan.Collect section.

These PSL processes are "attached" to the main Hardware Sentry icon (MS_HW_MAIN class) and not to the corresponding classes and instances.

No collection is performed on objects that have been paused.

When a device has been marked as "missing" by the discovery process (i.e. had been discovered and is no longer discovered), the collection process no longer queries the hardware information source and simply sets the status of the object to alarm.

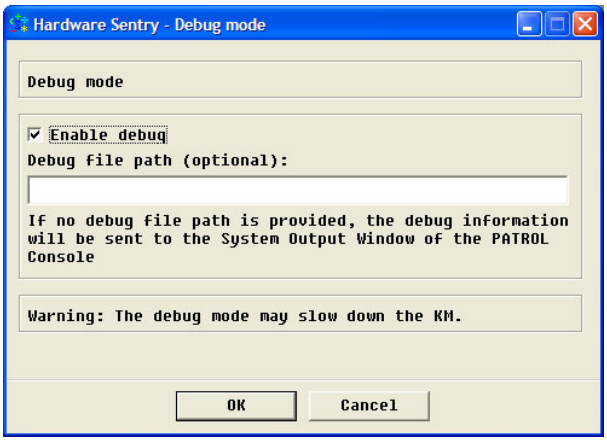
Section VI - Trouble-shooting

1 - Enabling the Debug Mode 57
2 - Reinitializing Hardware Sentry 58
3 - Hardware Sentry Shows Nothing 59
4 - Unable to See Temperature, Voltage or Fan 60
5 - Unable to See Disk Controller 61
6 - The CPU is overloaded 62

1 - Enabling the Debug Mode

By default, Hardware Sentry sends only the most critical information, warning and error messages to the System Output Window of the PATROL Consoles. Most often, this information is accurate enough to ensure that Hardware Sentry is properly working.

If you encounter a bug and wish to report it to Sentry Software, you will be asked to enable the Debug Mode and provide the debug output to the Sentry Software support team.


Hardware Sentry - Debug mode
Debug mode
Enable debug
Debug file path (optional):
If no debug file path is provided, the debug information will be sent to the System Output Window of the PATROL Console
Warning: The debug mode may slow down the KM.
OK
Cancel

To enable the debug mode, [right-click] the main Hardware Sentry icon, [KM Commands] > [Options] > [Debug...]

Check the "Enable debug" box.

By default, Hardware Sentry sends its debug output to the System Output Window of the PATROL Consoles.

When debugging the detection or discovery process of Hardware Sentry at the starting time of the Agent, some debug information may be lost by the PATROL Console as it is not yet connected to the PATROL Agent. In other cases, or when you want to trace the activity of Hardware Sentry during a few minutes, some debug information may be lost by the PATROL Console because its buffer is full.

In these cases, it can be useful to send the debug output of Hardware Sentry to a specified file.

Note: that debug file is stored on the computer where the Agent is running

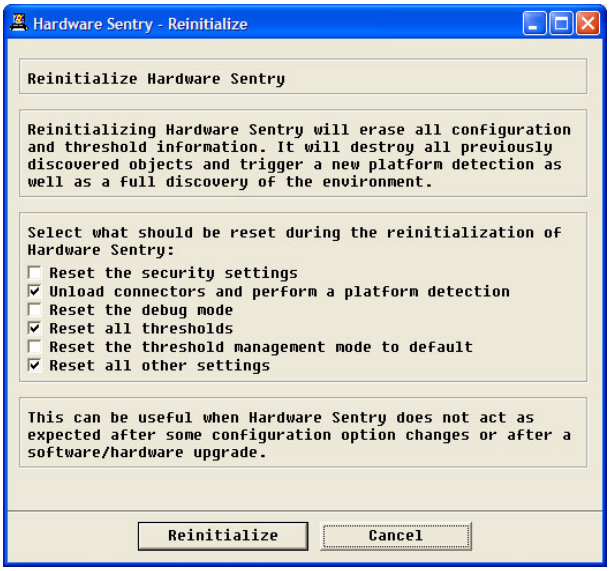
Warning! Pay attention to the file size -the debug output of Hardware Sentry could be very large when running for several days.

2 - Reinitializing Hardware Sentry

In cases Hardware Sentry is not properly functioning - creating missing devices you know are present, or not detecting several devices as it should, it is possible to reinitialize the configuration and let Hardware Sentry re-start the monitoring from scratch.

Hardware Sentry will then run a full discovery and will detect the computer's environment, set the appropriate connectors and re-start the monitoring of existing devices. Thresholds will be set to default so all previously manually set thresholds will be lost.

Note: After reinitializing Hardware Sentry it is not possible to go back to the previous configuration and so all changes will be lost.


Hardware Sentry - Reinitialize
Reinitialize Hardware Sentry
Reinitializing Hardware Sentry will erase all configuration and threshold information. It will destroy all previously discovered objects and trigger a new platform detection as well as a full discovery of the environment.
Select what should be reset during the reinitialization of Hardware Sentry:
Reset the security settings
Unload connectors and perform a platform detection
Reset the debug mode
Reset all thresholds
Reset the threshold management mode to default
Reset all other settings
This can be useful when Hardware Sentry does not act as expected after some configuration option changes or after a software/hardware upgrade.
Reinitialize
Cancel

To Reinitialize Hardware Sentry, right-click the computer icon and select "Reinitialize" from the menu.

You can select which settings of Hardware Sentry need to be reset. Select all options if you think that you made some configuration errors.

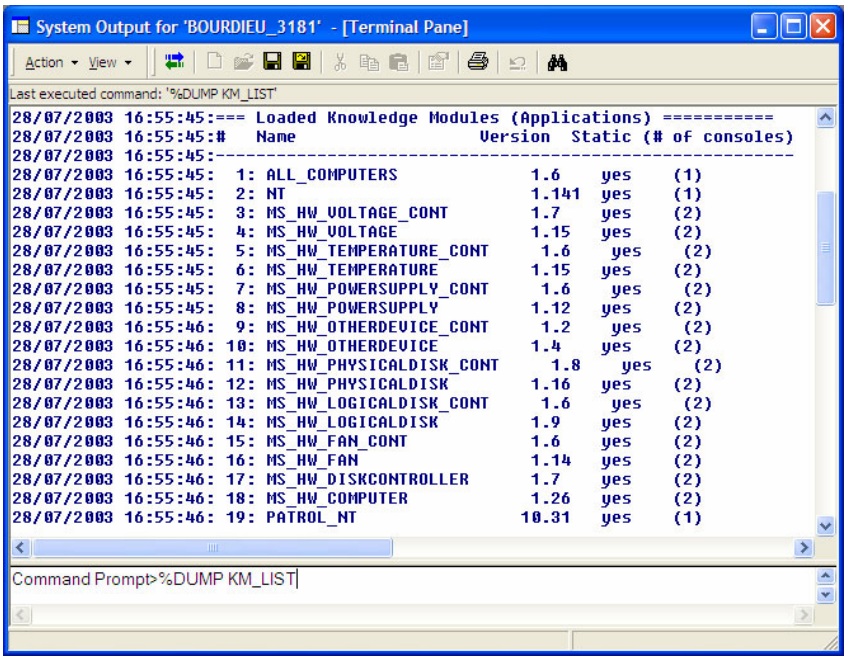
Click on the [Reinitialize] button to proceed or the [Cancel] button to cancel.

3 - Hardware Sentry Shows Nothing

Even if Hardware Sentry is unable to detect any available hardware information source, it should create an icon labeled "Hardware Sentry" under the main computer PATROL icon.

If no Hardware Sentry related information is shown at all in the PATROL Console, it means that Hardware Sentry is not running on the Agent, or that an internal error occurred.

Execute the **%DUMP KM_LIST** command in the System Output Window of the PATROL Console. This should produce the following output:


System Output for 'BOURDIEU_3181' - [Terminal Pane]
Action View
Last executed command: '%DUMP KM_LIST'
28/07/2003 16:55:45:=== Loaded Knowledge Modules (Applications) ===========
28/07/2003 16:55:45:# Name Version Static (# of consoles)
28/07/2003 16:55:45:----------
28/07/2003 16:55:45: 1: ALL_COMPUTERS 1.6 yes (1)
28/07/2003 16:55:45: 2: NT 1.141 yes (1)
28/07/2003 16:55:45: 3: MS_HW_VOLTAGE_CONT 1.7 yes (2)
28/07/2003 16:55:45: 4: MS_HW_VOLTAGE 1.15 yes (2)
28/07/2003 16:55:45: 5: MS_HW_TEMPERATURE_CONT 1.6 yes (2)
28/07/2003 16:55:45: 6: MS_HW_TEMPERATURE 1.15 yes (2)
28/07/2003 16:55:45: 7: MS_HW_POWERSUPPLY_CONT 1.6 yes (2)
28/07/2003 16:55:45: 8: MS_HW_POWERSUPPLY 1.12 yes (2)
28/07/2003 16:55:46: 9: MS_HW_OTHERDEVICE_CONT 1.2 yes (2)
28/07/2003 16:55:46: 10: MS_HW_OTHERDEVICE 1.4 yes (2)
28/07/2003 16:55:46: 11: MS_HW_PHYSICALDISK_CONT 1.8 yes (2)
28/07/2003 16:55:46: 12: MS_HW_PHYSICALDISK 1.16 yes (2)
28/07/2003 16:55:46: 13: MS_HW_LOGICALDISK_CONT 1.6 yes (2)
28/07/2003 16:55:46: 14: MS_HW_LOGICALDISK 1.9 yes (2)
28/07/2003 16:55:46: 15: MS_HW_FAN_CONT 1.6 yes (2)
28/07/2003 16:55:46: 16: MS_HW_FAN 1.14 yes (2)
28/07/2003 16:55:46: 17: MS_HW_DISKCONTROLLER 1.7 yes (2)
28/07/2003 16:55:46: 18: MS_HW_COMPUTER 1.26 yes (2)
28/07/2003 16:55:46: 19: PATROL_NT 10.31 yes (1)
Command Prompt>%DUMP KM_LIST

- If no MS_HW_MAIN entry is present, it means that Hardware Sentry is not loaded on the agent.
- Make sure that the “MS_HARDWARE_SENTRY1.kml” file is preloaded by the PATROL Agent and loaded by the PATROL Consoles, and that the “MS_HW_*.km” are not disabled.

  See the BMC Software documentation (*PATROL Agent Reference Manual*) to find out how to load a KM on the PATROL Agent.
- If the “MS_HW_*” classes are properly loaded and no icon appears in the PATROL Console, it probably means that the Hardware Sentry KM for PATROL has not been properly installed on the PATROL Agent.
- Re-install the KM and ensure that all files are properly installed (typically “*.lib” files in the “`%PATROL_HOME%\lib\psl folder`”)

4 - Unable to See Temperature, Voltage or Fan

The fact that the main Hardware Sentry icon is present but no temperature/voltage/fan information is shown may be caused by three issues:

- Hardware Sentry did not detect any hardware information source that is able to show the temperature/voltage/fan data. Typically, the vendor-specific hardware monitoring agent that comes with the server has not been properly installed.
- Hardware Sentry properly detected the vendor-specific hardware monitoring agent that comes with the server, but this agent is unable to provide any temperature/voltage/fan information. Please check that all the vendor-specific software is up-to-date (the hardware agent itself, the BIOS of the motherboard, the BIOS of other components like management processor if any, etc.)
- No temperature/voltage/fan sensor is provided with the computer (on a few Sun servers, all HP-UX systems and most of the IBM RS/6000 computers).

5 - Unable to See Disk Controller

On some computers, the vendor-specific hardware monitoring agent is only responsible for the monitoring of the baseboard: temperatures, fans, voltages and power supplies.

In this case, the disk monitoring is handled by the disk controller manufacturer. Therefore, you need to install additional software for your disk monitoring.

Please contact your server vendor to know which software must be used with your disk controller.

6 - The CPU is overloaded

Hardware Sentry has been optimized in order to use as few system resources as possible (CPU, memory, disk and network). As it does not process megabytes of data, Hardware Sentry should not overload your system. Hardware Sentry typically uses about 4 percent of the processor's time.

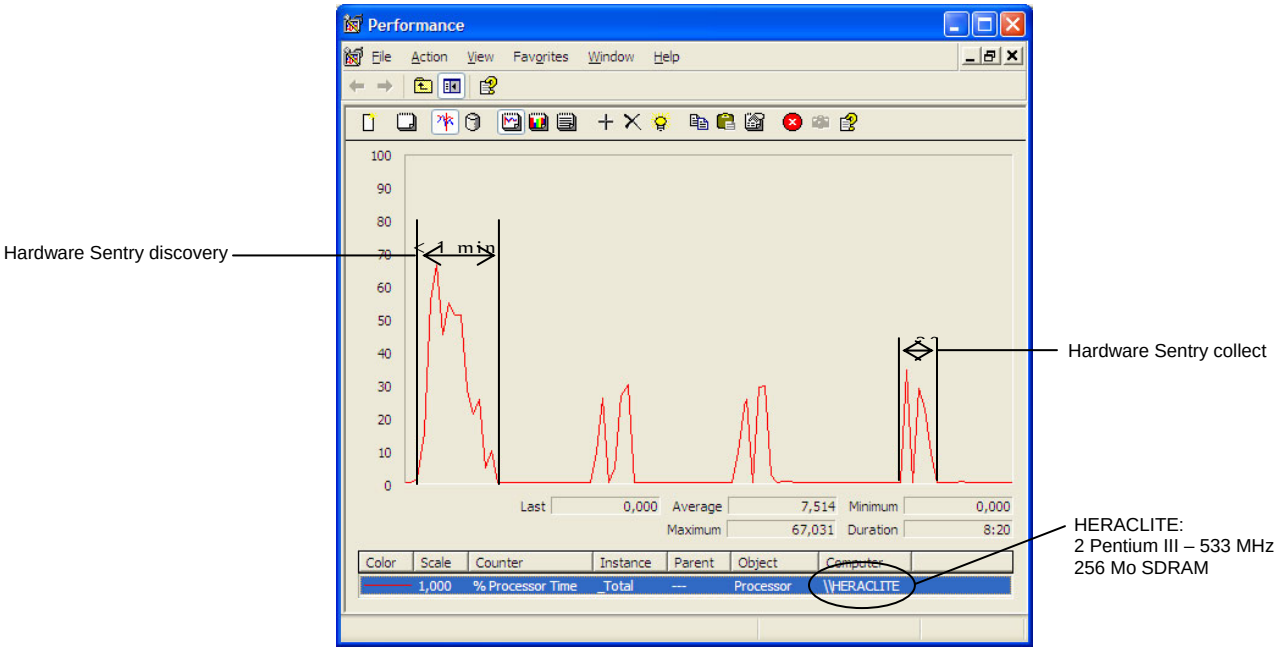
To diagnose if Hardware Sentry uses too much processor time, check which processes are overloading your CPU.

Hardware Sentry is a module that runs "inside" the PATROL Agent. Therefore, you should check the "*PatrolAgent.Exe*" process. But keep in mind that Hardware Sentry is not the only KM that runs on your PATROL Agent. Additionally, Hardware Sentry may spawn the following processes:

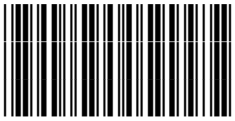
Operating system	Processes that Hardware sentry may be spawn
Under Windows	CSCRIPT.EXE MS_HW_MBMClient.EXE SW_ProcessList.Exe SW_ServiceInfo.Exe
Under Sun Solaris	prtdiag lom iostat awk, grep, sed
Under Linux	cimcli mii-tool ethtool
Under HP-UX	diskinfo ioscan lanscan pvdisplay awk, grep
Under AIX	lsdev errpt entstat lspv

If the "*PatrolAgent.Exe*" process takes all the processor time, disabling Hardware Sentry in the agent configuration ("`/AgentSetup/disabledKMs`") is a good way to find out if Hardware Sentry is the problem. If the "*PatrolAgent.Exe*" does not overload the CPU anymore, it probably means that Hardware Sentry is responsible for this overload.

If the "*PatrolAgent.Exe*" process and the other Hardware Sentry processes listed above are not consuming the processor time, disabling Hardware Sentry may help you find out if the vendor-specific hardware monitoring agent is responsible of this overload. In such a case, Hardware Sentry appears to be responsible for this CPU overload but only because it is querying faulty software. Therefore you should check for updates of your vendor-specific hardware monitoring software.



Notes



60208